NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ACHIEVING INTELLIGENCE PROLIFERATION: POLICIES AND PROGRAMS FOR LEVERAGING INTELLIGENCE SUPPORT TO STATE, LOCAL AND TRIBAL LAW ENFORCEMENT

by

James A. Dahl

December 2008

Thesis Advisor:	Robert Simeral
Co-Advisor:	Harold Trinkunas

Approved for public release: distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Achieving Intelligence Proliferation: Policies and Programs for Leveraging Intelligence Support to State, Local and Tribal Law Enforcement.	5. FUNDING NUMBERS
6. AUTHOR(S) CPT James A. Dahl	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release: Distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT

The need to proliferate intelligence to all appropriate levels of society is an imperative that has been all to vividly illustrated by the attacks of 9-11. Terrorism cuts across all levels of society through loss of life, economic chaos and inhibiting freedoms. The horrific loss of life cannot be minimized or discounted, but the damage goes further and its effects are enduring. Estimates of the future economic impact of terrorism, based on 9-11 losses, range from 100 million to 100 billion dollars per year. These numbers don't quantify the emotional toll or the self-imposed loss of personal freedom that attacks the very nature of democracy. The prolific nature of terror calls for an equally prolific response. This thesis has argued that in order to proliferate the intelligence, that will connect the dots and mitigate future terror attacks, all aspects of the intelligence enterprise must leveraged to form a collaborative intelligence community that includes federal, state and local law enforcement as well as private sector partners. The policies and programs examined identify information sharing as the chief enabler of leverage. The premise is that the more information shared the more intelligence is produced. This positive relationship drives the concept of intelligence proliferation.

14. SUBJECT TERMS Information Sharing, Intelligence, Fusion Centers, Intelligence led Policing, Homeland Security, Intelligence Proliferation	15. NUMBER OF PAGES 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release: distribution is unlimited

ACHIEVING INTELLIGENCE PROLIFERATION: POLICIES AND PROGRAMS FOR LEVERAGING INTELLIGENCE SUPORT TO STATE, LOCAL AND TRIBAL LAW ENFORCEMENT

James A. Dahl
Captain, United States Army
B.A., Elon College, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2008**

Author: James A. Dahl

Approved by: Robert Simeral
Thesis Advisor

Harold Trinkunas, Ph.D.
Co-Advisor

Harold A. Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The need to proliferate intelligence to all appropriate levels of society is an imperative that has been all to vividly illustrated by the attacks of 9-11. Terrorism cuts across all levels of society through loss of life, economic chaos and inhibiting freedoms. The horrific loss of life cannot be minimized or discounted, but the damage goes further and its effects are enduring. Estimates of the future economic impact of terrorism, based on 9-11 losses, range from 100 million to 100 billion dollars per year. These numbers don't quantify the emotional toll or the self-imposed loss of personal freedom that attacks the very nature of democracy. The prolific nature of terror calls for an equally prolific response. This thesis has argued that in order to proliferate the intelligence, that will connect the dots and mitigate future terror attacks, all aspects of the intelligence enterprise must leveraged to form a collaborative intelligence community that includes federal, state and local law enforcement as well as private sector partners. The policies and programs examined identify information sharing as the chief enabler of leverage. The premise is that the more information shared the more intelligence is produced. This positive relationship drives the concept of intelligence proliferation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is the product of the efforts of numerous people whose help, guidance and support made the end product possible. I would like to thank LTC (Ret.) Jeffery K. Toomer for affording me the opportunity to attend graduate school and the mentorship he provided me as young officer.

Thank-you to my advisors Robert Simeral and Harold Trinkunas for the guidance and direction, it was integral to the completion of this thesis. I especially appreciate your tolerance for my lack spelling and grammatical prowess. On that note, I would like thank Dawn for all of her hard work editing this document. I hope this unedited acknowledgement doesn't embarrass you too badly. I owe a debt of gratitude to Chief Scott Berg and Chief Tim O'Hara of the Anaheim Fire Department for the insight and introductions you provided me during my research. I would also like to thank Chief Pat Miller of the Ventura Ca. police department for his research and assistance.

Most importantly I would like to thank my wife, Carla, for her unwavering love and support, not only during this process but also throughout my 20 plus, and counting, years in the military. I love you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MAJOR RESEARCH QUESTION

> How can intelligence policies and programs at all levels of government be leveraged in support of state, local and tribal stakeholders in order to enhance National Security?

Maintaining and ensuring national security is the prime motivator for state action on the international stage. One method that states have traditionally used to ensure their security is deterrence. Deterrence is achieved through a proactive implementation of policies designed to keep non-citizens from violating the sovereignty of our Nation, thereby enabling national security. The arrival of terrorism on U.S. soil and its ensuing fatalities was a rude awakening. The asymmetrical nature of this new threat has raised some serious questions about the security of our borders. Security is achieved through a variety of means including physical and virtual barriers, and procedural and policy mitigations, all of which are supported by the nation's intelligence apparatus. To that end, the Department of Homeland Security (DHS) was created in the wake of the 9-11 attacks. The DHS mandates include the following:

> …Leading the unified national effort to secure America. It will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. It will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce.[1]

This is a tall order, and its level of efficacy will be largely influenced by the intelligence support rendered to state, local and tribal law enforcement agencies. Private sector partners will need to be engaged as well. This thesis will examine how current and proposed polices and programs support the leveraging of

[1] Department of Homeland Security, "Preserving our Freedoms, Protecting America," http://www.dhs.gov/index.shtm (accessed 6/12/2008).

intelligence assets to support SLTP. The DHS is a logical choice to take the lead in the effort to engage SLTP stakeholders as a force multiplier in the battle for national security.

B. IMPORTANCE

Homeland Security Presidential Directive 2 recognizes that terrorists attempt entry into the United States in order to engage in acts of terror or criminal enterprise The President directed the formation of a foreign terrorist tracking task force with the following mission:

> To aggressively prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.[2]

This task force was to be headed up by the Attorney General and included personnel from across federal law enforcement agencies and the intelligence community. Notably absent from this presidential directive is any explicit participation by SLTP stakeholders. Their sheer numbers when compared to the personnel assets available to the federal government underscores the importance of SLTP as equal partners. As of 2004, the Department of Justice reported 17,876 total state and local law enforcement agencies employing 731,903 sworn officers.[3] This number represents almost seven times the number of non-military federal employees with arrest powers. Furthermore, inclusion of first responders and private sector entities increases the number of potential partners by orders of magnitude.

There are three interrelated areas impacted by the leveraging of intelligence assets. They are border security, criminal activity, and terrorism. The

---

[2] George W. Bush, "Weekly Compilation of Presidential Documents," *Weekly Compilation of Presidential Documents* 37, no. 44 (November 5, 2001,), 1561, http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=2001_presidential_documents&docid=pd05no01_txt-8.pdf (accessed 3/19/2008).

[3] Bureau of Justice Statistics, “Law Enforcement Statistics”,http://www.ojp.gov/bjs/lawenf.htm (accessed 9/17/2008, 2008).

southern border of the United States provides a snapshot of the magnitude of the problem. In 2005, 1,200,000 illegal aliens were captured crossing the southern border of the United States without proper authorization.[4] The lions' share were Mexican nationals, however, some 150,000 were other nationalities. U.S. Customs and Border Protection (CBP) estimates it apprehends only one in four; this means that some 450,000 individuals, who were not Mexican, entered the country across our southern border in 2005. It is prudent to assume that they are not all here for acceptable reasons, such as seasonal employment or political asylum, and some may pose a threat to national security by engaging in unlawful activity. Proper leveraging of intelligence assets can be vital to help ascertain the identity and intentions of these individuals.

Terrorism is at the forefront of American consciousness due to the events of 9-11, but there are other national security dilemmas that will remain, even if the terrorist threat is mitigated. DHS' Under Secretary for Intelligence, Charles Allen, has identified several of these additional areas of concern. He testified to the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Homeland Security Committee:

> The United States and its allies are engaged in a continuing, global struggle against a broad range of transnational threats. Our nation's communities face the threat of terrorism, of cross-border violence fomented by illicit narcotics trafficking and alien smuggling, and other threats apart from terrorism.[5]

Secretary Allen was eluding to an illicit economy of crime and violence, that, were it a nations' gross national product, would be the size of Spain.[6] There is a positive relationship between crime and terrorism. Terrorism requires capital and infrastructure in order to be successful. The capitalist nature and open

---

[4] Global Security, "US-Mexico Border Fence: Great Wall of Mexico," http://www.globalsecurity.org/security/systems/mexico-wall.htm (accessed 3/8/2008, 2008).

[5] Homeland Security, *Statement of Assistant Secretary Charles E. Allen,* 2007.

[6] Moises Naim, "The Five Wars of Globalization," *Foreign Policy*, no. 29, January (2003), http://www.foreignpolicy.com/Ning/archive/archive/134/5wars.qxd.pdf (accessed 6/12/2008).

society of the United States provides terrorists with the means to engage in the criminal acts necessary to underpin their sustainability. The intermingling of crime and terrorism makes the methodology for fighting crime a feasible strategy for fighting terrorism. Therefore it is important that intelligence assets held at the federal level are used to support SLTP stakeholders, especially law enforcement with a direct interest in national defense. If the United States is going to enjoy a continued high standard of living, the paradigm must shift from federally provided national security to full and equal partnership with SLT law enforcement agencies. These agencies will become second or third tier assets without appropriate intelligence support.

C. PROBLEMS AND HYPOTHESES

This thesis will answer how intelligence policies and programs at all levels of government can best be leveraged to support SLTP stakeholders in order to support national security. The engagement of all stakeholders in a collaborative intelligence enterprise is vital to national security; especially given the 9-11 hijackers entered the country by largely legal means under the radar of traditional intelligence structures. The current state of border security and immigration policy allowed them slip through the cracks by marginalizing those most able to fill those cracks, SLTP entities. Methodologies for identifying potential terrorists and taking appropriate action without compromising the rights of citizens are problematic. The historical lack of focus on terrorism has resulted in an inability to effectively apprehend terrorists. There are arguments that the lack of terrorist attacks since 9-11 shows the salient value of current policy. This argument attempts to prove a negative. The unquantifiable nature of counter terrorism makes new policies a hard sell to a complacent public. In order to insure security, the civil sector must see the value of new programs, such as fusion centers, at the local level. One way to achieve this goal is through collaboration between intelligence and law enforcement. This country is well-versed in law enforcement techniques and has the pieces in place to conduct effective operations in both law enforcement and counter-terrorism arenas. If we can integrate federal

agencies and SLTP and enable them to focus on the nexus of crime and terror, then the chances of apprehending future terrorists before they act will increase. The ability to do this depends heavily on intelligence support.

Intelligence support needs to cover a broad spectrum of interlocking pieces that make up the puzzle of national security. The brick and mortar pieces include fences and walls, such as a border fence in the San Diego region. A more robust barrier is under construction in San Diego pursuant to the secure fence act of 2006.[7] The new fence will use technology to supplant the physical with the virtual in many areas. Unmanned Aerial Vehicles (UAVs), video surveillance, and motion sensors are only a few of the technological pieces that will require the input and support of intelligence agencies. Technology is not a panacea for national defense; instead it must be an enabler of human interaction. Interagency cooperation and a shift in intelligence culture must be addressed in order for any effort to be successful. The statutory constraints of checks and balances restrict the way that intelligence can be collected, analyzed and consumed by domestic agencies. The mitigation of cultural constraints must be addressed, along with funding and technology, if the DHS is going to succeed in its mandate. Leveraging intelligence support, by DHS to stakeholders, whether federal, state, local, tribal, or private sector will buttress national security and allow for a powerful projection of the nation's policies at our borders.

D. LITERATURE REVIEW

The United States currently uses the approach of an active layered defense that is designed to defeat a potential enemy as far from our borders as possible. James Carafano sees some flaws with this system. The construct of interlocking layers, each backing up another, leads to an imperfect system filled with gaps, which can be exploited by those who would enter the nation illegally.

[7] "Secure Fence Act of 2006," http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6061enr.txt.pdf (accessed 6/12/2008).

He instead advocates a system of systems.[8] The goal of this system would be the integration and modification of disparate methodologies and organizations to create symbiosis. This integration illustrates the need for structures where intelligence, law enforcement, and SLTP stakeholders can interact in meaningful ways. The nature of the intelligence support provided by DHS to SLTP will be a critical factor in the development of this relationship.

Magnus Ranstorp, a lecturer at the University of Saint Andrews and recognized Hezbollah expert, characterizes the new terrorist threat as one that both embraces technology and also uses the simplest means to defeat it. In his testimony to the 9-11 commission, he noted that:

> Despite our asymmetry in power projection both militarily and economically, the reality is that modern, high tech and complex societies can be brought to its knees by simple attacks against critical nodes that constitute their very strength…a main lesson of September 11th is that in an interdependent world, no one is invulnerable.[9]

The notion that society can be brought to its knees by attacking critical nodes recognizes the networked nature of the nation's critical infrastructure (CI). The networked structure of CI is not well served by the decentralized structure of American law enforcement. Ranstorp offered 10 areas of focus in order to form an effective counter terrorism strategy. Many of them relate directly to exploiting the nexus of crime, border security, and intelligence.

Terrorists use false or stolen identities both to move unhindered from place to place and to secure financing. The average number of identities possessed by arrested al-Qaeda operatives is 16, coupled with a like number of

---

[8] James Carafano, "Safeguarding America's Sovereignty: A "System of Systems" Approach to Border Security," http://www.heritage.org/research/homelandsecurity/bg1898.cfm (accessed 3/7/2008).

[9] National Commission on Terrorist Attacks Upon the United States, *Statement to the National Commission on Terrorist Attacks upon the United States,* 2003, http://govinfo.library.unt.edu/911/hearings/hearing1/witness_ranstorp.htm (accessed 6/12/2008).

credit cards.[10] In addition to making them hard to detect, once apprehended, the investigation is delayed while trying to establish a real identity. Ranstrop advocates an intelligence-led approach to law enforcement before acts of terror or associated crimes can occur. Intelligence Led Policing (ILP) is a methodology that takes the everyday bits of information collected by local law enforcement and analyzes and integrates them into informative law enforcement intelligence reports. The bottom of line of ILP is analysis and dissemination. ILP will be discussed in depth later in this thesis.

The states ability to improve the receipt, gathering, analysis, and sharing of travel intelligence data will be necessary to secure our borders. One current DHS program that addresses the need for traveler intelligence is U.S.-Visit. The US-Visit program is the centerpiece of the United States government's efforts to transform our nation's border management and immigration systems in a way that meets the needs and challenges of the 21st century.[11] The program is designed to provide a layered approach to security by integrating the visa application, entry, and exit procedures into a process that shares information in order to facilitate national security. The U.S.-Visit program has been implemented in stages and remains incomplete. U.S.-Visit is an invaluable intelligence-gathering tool that enables us to identify those that overstay their visas and take appropriate action. The biometric aspect of the U.S.-Visit program provides the ability to verify that people are whom they say. This capability reduces fraud and makes terrorist watch lists all the more effective. U.S.-Visit entry procedures went "on line" in January 2004. By March of 2008, the entry program had screened over 112,000,000 people. This has resulted in some 3000

---

[10] National Commission on Terrorist Attacks Upon the United States, *Statement to the National Commission on Terrorist Attacks upon the United States,* 2003, http://govinfo.library.unt.edu/911/hearings/hearing1/witness_ranstorp.htm (accessed 6/12/2008).

[11] Department of Homeland Security, "US-VISIT Program," http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed 4/26/2008).

people being denied entry to the country.[12] The private sector is a key partner in this program, as the onus for its final implementation has been placed on the air carriers themselves. One important way the DHS can leverage intelligence is to ensure the full implementation of the system and the dissemination of the data to law enforcement agencies.

> DHS has provided more than $380M to state and local governments…the department, along with other federal partners, has also dramatically improved the quantity and quality of analytical intelligence products that are provided to state and local governments.[13]

The preceding is an excerpt from a DHS news release and appears to show that DHS support to SLTP is progressing at an acceptable rate. This is the case across the board. A 2006 survey of the 55 state homeland security directors found that more that half of the respondents were dissatisfied at some level with the specificity and actionable quality of the intelligence they received from the federal government.[14] Two of the issues they cited were a lack of “tear line” intelligence products and a perception that policies and procedures were forced upon them without prior consultation or consent. In a related question, the inflexibility of DHS grant money was cited as major contributor to friction between the DHS and states. An unidentified survey respondent made the following comment, which was echoed by the overall results:

> The best action DHS could take to benefit the security of the state…would be to allow for more flexibility for expenditure of the Homeland Security grants.[15]

---

[12] Federal Register, "FR Doc E8-8956”, Volume73, Number 80,April 24, 2008, http://edocket.access.gpo.gov/2008/E8-8956.htm (accessed 5/9/2008).

[13] Department of Homeland Security, "DHS Strengthens Intel Sharing at State and Local Fusion Centers," news release, July 27, 2006, http://www.dhs.gov/xnews/releases/press_release_0967.shtm (accessed 6/19/2008).

[14] NGA Center for Best Practices, "2006 State Homeland Security Directors Survey," http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf (accessed 6/19/2008).

[15] Ibid.

The survey seems to point to a need for greater interaction between DHS and SLTP officials, as well as funding support and attention to classification issues. It also suggests that funding for intelligence specific endeavors, such as additional intelligence analysts, could be an appropriate support response from the DHS to address the SLTP needs.

The National Governors Association (NGA) issued its policy position (EC-05) paper on Homeland Security in July of 2007. EC-05 addressed some specific intelligence issues and echoed the survey participants' frustration with classification issues. Additionally, the NGA advocated federal intelligence liaisons in state fusion centers and called for expedited issuance of security clearances to SLTP personnel.[16] The DHS is attuned to the needs of the states, and as of March 2008, there were 58 operational intelligence fusion centers in the United States receiving some sort of intelligence support from the DHS.[17] This evolved recently with the fielding of DHS personnel to limited sites. As of March 2008, there were 23 intelligence officers assigned to fusion centers, with more in the pipeline.[18] . The DHS sees four distinct benefits arising from fusion centers. These benefits are applicable to all stakeholders participating in the fusion process. They include clearly defined information gathering requirements, improved intelligence analysis and production capabilities, improved information and intelligence sharing, and improved prevention, protection, response and recovery capabilities[19]

---

[16] National Governors Association, "EC-05 Homeland Security Policy," July, 24, 2007, http://www.nga.org/portal/site/nga/menuitem.8358ec82f5b198d18a278110501010a0/?vgnextoid=2a6a9e2f1b091010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD (accessed 6/19/2008). 2.

[17] Department of Homeland Security, "State and Local Fusion Centers," http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed 9/17/2008).

[18] Ibid.

[19] John Rollins, "Fusion Centers: Issues and Options for Congress," Report for Congress (Congressional Research Service),http://www.fas.org/sgp/crs/intel/RL34070.pdf (accessed 11/2/2008, 2008).

Despite integration efforts, the current state of intelligence support to law enforcement is like that of a vacuum. The perception is that the DHS and other federal agencies are sucking up information from the state, local and tribal government levels, while providing very little in return. The entire concept of homeland defense is an inductive, self-help construct. The vacuum analogy does not allow for two-way flow; nor does it encourage the lateral sharing of information.

Movement across all axes in all directions will be required to solve issues as diverse as those presented by the whole of national security. In short, the system is stove piped when it needs to be networked.

E. METHODS AND SOURCES

In order to identify shortcomings, it is necessary to establish a baseline from which to work. Once the baseline is established, gaps between what is official policy and the "ground truth" will be revealed. The nature of these gaps will be of paramount importance for the identification of solutions. To establish the ground truth, the nature of the Intelligence Community is explored; its evolution, or lack thereof since 9-11, and its interaction with SLTP is traced. The research will be accomplished via a thorough review and examination of pertinent policy documents. These documents will come from Congressional Research Service, the Department of Homeland Security and other official sources from across the IC. The polarizing nature of national security has made it a relevant topic for academics and journalists' alike, so professional journals and popular media are sourced as well, in order to gain perspective from outside government circles. The study has little to no statistical component as the thesis deals primarily with policy issues whose metrics are hard to define. This thesis contains a study of federal strategies and how they affect SLTP and the state of national security. A case study consists of the perceptions of SLTP partners in the City of Anaheim, California.

The end result of this analysis is the identification of gaps pertaining to intelligence support. These gaps likely fall in three key areas: financial support, analysis and administrative issues such as classification and interagency coordination. The case study will serve as the baseline to evaluate current and proposed policies and programs and identify gaps. Once the gaps are identified, it is my intent to suggest ways that the DHS intelligence apparatus can best leverage support to SLTP law enforcement officials. The end result of this support should be the proliferation of intelligence that bolsters national security in a meaningful way.

F. STRUCTURE OF THE THESIS

1. Setting the Table

This chapter will "set the table" by covering the structure and history of the IC, the intelligence cycle, various statutory items such as the Patriot Act and IRTPA, and some barriers to leveraging intelligence. This background information is important for putting current intelligence related policies and programs into context. The concept of Intelligence Proliferation will be introduced as both an achievable goal and also an example of what the successful leveraging of intelligence will look like.

2. Framing the Problem

In order to identify the salient issues and the appropriate mitigations, the perceptions of SLTP stakeholders in California were gauged through surveys and individual interviews. The survey, conducted in 2005, consisted of respondents who were all law enforcement executives in California. The same respondents were polled again in 2007, and the results compared. In addition, personnel with the Anaheim California Homeland Security Battalion were interviewed in the fall of 2008. The results of this research served as a guideline for evaluating the efficacy of the policies detailed in this thesis.

3. Policies and Programs

This chapter contains a review of pertinent policies and programs. The items reviewed represent some of the best available policy and program tools for the achievement of intelligence proliferation. It concludes by identifying the commonalities between plans and suggests where the DHS should focus its energies and resources. The two areas that show the most promise are Intelligence Led Policing (ILP) and Fusion centers, which will be covered in a subsequent chapter.

4. The Promise of Proliferation

ILP and Fusion Centers represent the greatest promise for the leverage of intelligence assets and the achievement of intelligence proliferation. They are discussed in terms of background, barriers, benefits, and points of entry for DHS support and how they promote intelligence proliferation and, by extension, national security.

5. Backbrief

Conclusions and final thoughts for the way forward are presented here.

II. SETTING THE TABLE

A. WHAT IS INTELLIGENCE PROLIFERATION

The ultimate goal of the policies and procedures that will be examined in this thesis is intelligence proliferation (IP). Semantics are an important part of the discussion as the meanings of words change fundamentally with their employment. No single word in policy is as linguistically malleable as intelligence. Intelligence can be simultaneously used to refer to the Intelligence Community (IC) or the process used to derive strategic or tactical knowledge. The finished product disseminated in the intelligence process is often referred to by the same term. Mark Lowenthal defines intelligence as it relates to information:

> Information is anything that can be known…Intelligence refers to information that meets the stated needs of policy makers and has been collected, processed and narrowed to meet those needs…all intelligence is information; not all information is intelligence.[20]

Lowenthal's definition constrains the use of intelligence to the purview of policy makers, and that is in fact the major theme of his book from which the definition is drawn. This is a valid view given the traditional purposes of intelligence, which are avoiding strategic surprise, providing continuity of expertise in a fluid political landscape, supporting the policy process and maintaining secrets. The shift from nation-state based threats to asymmetrical non-state actor based threats has facilitated a need for the habitual use of intelligence at the SLTP level, including law enforcement personnel, first responders, and in many cases private industry. At this level, in a very tactical sense, intelligence consumption becomes the purview of decision makers, not policy makers. The need for tactical intelligence at the first line of defense is more than simply the one way flow of information from SLTP to the federal government, and it is more than reciprocity back down the chain. True

[20] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington DC: CQ Press, 2006), 6.

proliferation of intelligence lies in the omni-directional flow of information from all stakeholders, whether they are federal, state, local, tribal, first responder, or private industry. The disparate information must flow into the intelligence cycle and emerge as intelligence products for the consumption of all concerned. In order for this to happen, all stakeholders must be integrated into the intelligence process, not just as providers of raw data, but also as active participants. When everyone is involved as partners and the unique aspects and capabilities of each organization are leveraged for the common welfare and intelligence products are available for consumption by all, then we will have achieved intelligence proliferation. Intelligence proliferation is defined in this thesis as:

> INTELLIGENCE PROLIFERATION: A state of being, within the context of providing national defense, in which there is an omni-directional flow of information in and finished intelligence products out of the intelligence process. These products will be tailored to the specific needs of the consumer and can be either strategic or tactical. This omni-directional flow embraces the traditional IC, state, local and tribal officials, law enforcement, first responders, and private industry.

A discussion of the structure of the IC and how it currently interfaces with other levels of society is important in order to begin discerning how IP can be achieved.

B. THE STRUCTURE OF THE INTELLIGENCE COMMUNITY

The National Security Act of 1947 laid the foundations of the IC. Section II of the act provides the intent of the acts framers:

> In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security…[21]

[21] United States Congress, "National Security Act of 1947," http://www.intelligence.gov/0-natsecact_1947.shtml (accessed 9/5/2008).

Over time the membership and structure of the IC has evolved into the current structure of 16 primary members spanning 5 executive branch departments and the fundamentally independent Central Intelligence Agency. The oversight structure is rounded out by multiple funding streams and committees. This section will give a thumbnail sketch of the oversight, funding, and membership of the IC. An understanding of the sheer complexity of the IC structure is necessary if true efficiency is to be attained.

1. Oversight

The National Security Act of 1947 designated the Director Central Intelligence (DCI) as a dual-purpose post, which controlled not only the Central Intelligence Agency (CIA) but also acted as oversight to the entire IC.[22] The powers of the DCI were limited to the provision of guidance for budget preparation, the approval for the reprogramming funds across programs within the same department, and the transfer of funds and personnel between members of the IC.[23] On paper these powers appear to be substantial; the reality is that procedures for the application of these powers effectively negated the authority of the DCI. Title I of the Intelligence Reform and Terrorism Prevention act of 2004 (IRTPA) established the position of the Director of National Intelligence (DNI).[24] The new position of DNI relieved the DCI of the dual responsibilities held under the 1947 act. The DCI reverted to being solely responsible for the CIA and the DNI assumed oversight for the IC and primary briefing responsibilities for the President. The DNI gained a modicum of authority from the IRTPA through budgetary control of the National Intelligence Program (NIP) and the direct ear of the President with regard to the appointment of most IC members.

---

[22] United States Congress, "National Security Act of 1947," http://www.intelligence.gov/0-natsecact_1947.shtml (accessed 9/5/2008).

[23] Ibid.

[24] 108th US Congress, "Intelligence Reform and Terrorism Prevention Act of 2004," http://www.nctc.gov/docs/pl108_458.pdf (accessed 9/5/2008).

Of the 16 members of the IC, 15 report not only to the DNI, but also to cabinet level officials. The one exception is the CIA. The entire IC, however, is subject to oversight from the executive and legislative branches of government. The President's Foreign Intelligence Advisory Board is responsible for assessing the quality, quantity, and adequacy of intelligence collection, analysis, counterintelligence, and other activities of the IC.[25] The President's Intelligence Oversight Board conducts independent investigations as required and reviews the practices and procedures of the inspectors general and general counsels of the IC. The Office of Management and Budget is primarily responsible for reviewing budgets and vetting testimony based on the priorities and guidance of the President.

The legislative branch oversight apparatus includes the US Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). Other committees become involved as the activities of the IC members overlap into their areas of responsibility. The best example of this the House Armed Services Committee, which often is involved with intelligence oversight through the intelligence arms of its member services.

2. Funding

The funding of the IC comes from three primary sources. They are the National Intelligence Program (NIP), Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA) program. The members of the IC often receive funds from multiple streams depending into which category a specific agency program falls. The NIP deals primarily with programs that are not of a specific military nature. Notable IC members in this category are the CIA and DHS. Their funding stream accounts for over 50% of the total budget. JMIP, which accounts for roughly 10% of the budget, is concerned with ventures that cross service boundaries. The important oversight conundrum here

[25] "United States Intelligence Community," http://www.intelligence.gov/1who.shtml (accessed 9/5/2008).

is that DNI can only exercise budgetary constraint over the NIP. This effectively gives the Army, Navy, Marines and Air Force a free hand as they fall under TIARA funds, which account for 30% of the intelligence budget.[26]

3. Membership

There are 16 members of the traditional IC. This thesis will argue in part that in order to achieve Information Proliferation, the IC must embrace SLTP stakeholders as partners in a networked intelligence enterprise. A list and brief description of the current members follows.

National Security Agency (NSA): The NSA is widely regarded as the most powerful single member of the IC. Residing in the Department of Defense, NSA is the primary producer of signals intelligence (SIGINT) for the nation.[27]

National Reconnaissance Office (NRO): The NRO also falls under the purview of the DOD, but is funded through NIP. They are responsible for building and maintaining reconnaissance satellites. The activities and even the existence of the NRO was classified until 1992.[28]

National Geospatial-intelligence Agency (NGA): The NGA develops imagery and map-based intelligence (IMINT) solutions for U.S. national defense, homeland security and safety of navigation.[29]

Defense Intelligence Agency (DIA): Formed in 1961, the DIA is responsible for providing timely, objective, and cogent military intelligence to war

---

[26] William Lahneman, "The U.S. Intelligence Community," https://www.chds.us/coursefiles/NS4156/lectures/intel_us_intel_comm/player.html (accessed 9/5/2008).

[27] National Security Agency, http://www.nsa.gov/about/ (accessed 9/5/2008).

[28] National Reconnaissance Office, " http://www.nro.gov/ (accessed 9/5/2008).

[29] National Geospatial-Intelligence Agency, http://www1.nga.mil/Pages/Default.aspx (accessed 9/5/2008).

fighters, defense planners, and defense and national security policymakers.[30] They are 1 of 3 all source analysis agencies and take the lead in measurements intelligence (MASINT).

State Department's Bureau of Intelligence and Research (INR): The INR primarily supports the intelligence needs of the Department of State. They make sure that intelligence activities support foreign policy and national security objectives. They are the 2nd of three all source agencies.[31]

Federal Bureau of Investigation (FBI): The FBI has traditionally been a law enforcement agency with domestic responsibilities. The National Security Branch of the FBI was created, at the behest of the President, in 2005 to specifically counter the transnational terrorist threat.[32]

Department of Energy (DOE): The DOE is responsible for three areas that have a direct link to intelligence. They are in the business of insuring the integrity and safety of the country's nuclear weapons, promoting international nuclear safety and nuclear non-proliferation.[33]

Department of Treasury: The Department of Treasury Office of Terrorism and Financial Intelligence is responsible for marshalling the Treasury Department's policy, enforcement, regulatory, and intelligence functions in order to sever the lines of financial support to international terrorists, proliferators of weapons of mass destruction, narcotics traffickers, and other threats to our national security.[34]

---

[30] Defense Intelligence Agency, http://www.dia.mil/ (accessed 9/5/2008).

[31] Bureau of Intelligence and Research, http://www.state.gov/s/inr/ (accessed 9/5/2008).

[32] "Federal Bureau of Investigation Homepage," http://www.fbi.gov/ (accessed 9/5/2008).

[33] U.S. Department of Energy, "National Security," http://www.doe.gov/nationalsecurity/ (accessed 9/5/2008).

[34] Department of the Treasury, http://www.treasury.gov/ (accessed 9/5/2008).

Drug Enforcement Administration (DEA): The DEA is responsible for providing the IC with intelligence acquired while conducting its counter narcotics missions.[35]

Army, Navy, Air Force, Marines, and Special Operations Command: All of the services and the joint Special Operations command maintain organic intelligence capabilities which are tailored to their specific needs. Collectively they make up 5 members of the IC.

Defense Airborne Systems was an organization within the DOD from 1993 until 1998 when the Intelligence Authorization Act for FY 1998 (H.R. 1775) canceled its funding. DARO dealt with the “air breathing” IMINT platforms such as unmanned aerial systems (UAS). The predator UAS, representative of their work, was transferred to the Air Force and other responsibilities absorbed by DIA.[36]

The Coast Guard also maintains a robust intelligence capability that serves to support its border security and search and rescue missions. They are now a part of the Department of Homeland Security and will be considered as included during any discussion of DHS capabilities.

Department of Homeland Security (DHS): The DHS mission statement makes it clear that they are the lead agency for evaluating vulnerabilities and coordinating with other federal, state, local, and private entities to ensure the most effective response to all hazards of a national scope. The collection, protection, evaluation, and dissemination of information to the American public, state and local governments, and the private sector are central to this task.[37] The mandate to get quality intelligence into the hands of homeland security stakeholders will form a core competency of the organization.

---

[35] Drug Enforcement Administration, http://www.usdoj.gov/dea/index.htm (accessed 9/5/2008).

[36] Lahneman, *The U.S. Intelligence Community*

[37] Department of Homeland Security, "Information Sharing & Analysis," http://www.dhs.gov/xinfoshare/ (accessed 9/5/2008).

4. Legislation

The Patriot Act (H.R. 3162) was approved less than seven weeks after the attacks of 9-11. The speed at which the bill was written and passed suggests that many of the sections had been contemplated prior to 9-11. Many of the provisions were decried by organizations such as the American Civil Liberties Union (ACLU). Laura Murphy, the director of the ACLU, sent a letter to the Senate urging them to vote down the legislation on the basis that the powers granted to the Executive Branch and federal law enforcement went beyond what was necessary to fight terrorism.[38] Whether or not the bill was co-opted by opportunistic legislators for their own personal agendas will not be discussed in this thesis. What is important is that the compressed timeline and pre-positioned legislation resulted in a bill that was about more than terrorism and put some significant tools in the hands of law enforcement.

On March 9, 2006, President George W. Bush revisited the Patriot Act when he signed H.R. 3199, USA Patriot Improvement and Reauthorization Act of 2005. President Bush reiterated the importance of the nexus of crime and terror. Similarly he underscored the importance of interagency cooperation and intelligence sharing:

> The law allows our intelligence and law enforcement officials to continue to share information. It allows them to continue to use tools against terrorists that they used against -- that they use against drug dealers and other criminals. It will improve our nation's security while we safeguard the civil liberties of our people. The legislation strengthens the Justice Department so it can better detect and disrupt terrorist threats. And the bill gives law enforcement new tools to combat threats to our citizens from international terrorists to local drug dealers.[39]

---

[38] Laura W. Murphy, "American Civil Liberties Union: Letter to the Senate Urging Rejection on the Final Version of the USA PATRIOT Act," October, 23, 2001, http://www.aclu.org/natsec/emergpowers/14401leg20011023.html (accessed 10/1/2008).

[39] George W. Bush, "Comments upon Signing H.R. 3199, USA Patriot Improvement and Reauthorization Act of 2005," March, 9, 2006, http://www.whitehouse.gov/infocus/patriotact/ (accessed 10/1/2008).

If the nexus of crime and terror is a focal point for counterterrorism, then the nature of the IC must change. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) made several fundamental changes to facilitate the paradigm shift. As previously mentioned, the establishment of the DNI by Title I of the act was designed to more effectively integrate disparate agencies under a common chain of concern. IRTPA also mandated the Information Sharing Environment (ISE) that will be covered in detail later in this thesis. The act also established a civil liberties protection officer in order to insure that protections against the violations of rights are integrated into all policies and procedures.[40]

The combination of these two relatively new pieces of legislation with existing laws forms the framework within which the IC must work to ensure intelligence proliferation.

C. THE INTELLIGENCE CYCLE

Information is not intelligence. To become intelligence information must be processed. The classic intelligence production model is viewed as process with defined policies and procedures governing each step. There are some differing opinions as to the number of steps, but general agreement is between five and seven. I will examine the intelligence cycle as a seven-step process. The ideal outcomes of the process are targeted, actionable intelligence products. There is a positive relationship between the value of intelligence to a given user and the input that consumer had in the generation process. In order facilitate this positive relationship, SLTP stakeholders must be integrated into a process that has generally been the purview of professional federal agencies. A discussion of the intelligence cycle is needed to understand the points of entry that will be most useful to SLTP stakeholders. The seven steps are adopted from Lowenthal's

[40] *Intelligence Reform and Terrorism Prevention Act of 2004* , Title I sec 1016, 1061

book, *Intelligence: from Secrets to Policy.* The steps, briefly described below, are the identification of requirements, collection, processing/exploitation, analysis/production, dissemination, consumption, and feedback.[41]

1. Requirements

The production of intelligence is resource intensive. Given that there are finite amounts of time, money, personnel and physical assets, stakeholders must make hard choices about exactly how these limited resources are to be expended for maximum return. The validity of a requirement is driven by the consequence of a given event. At the national level, the National Intelligence Priorities Framework (NIPF) adjudicates the debate between high probability low impact events and low probability high impact events. The NIPF receives a semiannual review in order to ensure the most urgent needs are being met, and it is used as a guide for the budget process.[42] The local first responder is not concerned with what happens in a cave in Afghanistan. To make the SLTP stakeholders viable partners in national security, the intelligence provided needs to illustrate a direct nexus to their community. It is unrealistic to have representatives of every community in the United States occupying a desk at the National Operations Center. The specific needs of the local community need a place to interface with requirements generation. My research suggests that the appropriate venue for this discourse is at regional fusion centers.[43] Fusion centers will be explored in detail in Chapter IV.

2. Collection

Once a requirement has been validated, the task of collecting information begins. Not every requirement is fulfilled in the same manner. This needs to be a capability-based process. The STLP stakeholder needs only to define the

---

41 Lowenthal, *Intelligence: From Secrets to Policy*, 54.

42 Ibid., 58.

43 Scott Berg, Personal interview by the author, 09/23/2008.

requirement and let the collection assets determine the best way to achieve it. There are five generally recognized types of intelligence that intuitively suggest how the information that generates them is to be collected, though the capabilities mentioned are only representative and in no way are all-inclusive. The first three are highly technical and expensive. Image Intelligence (IMINT) is just that - images. It has evolved from simple photographs to infrared and satellite imagery. Signal Intelligence (SIGINT) is the discipline that includes everything from intercepting phone conversations to the use of radar tracking. Measurement and Signatures Intelligence (MASINT) detects things such as radiation, important given issues of nuclear weapons proliferation and the emissions of gases into the atmosphere. A less technical method is Human Intelligence (HUMINT). This discipline involves what people view as the classic “007” type of espionage. The newest player on the scene is Open Source Intelligence (OSINT). In the past this meant reading the newspaper of your enemy. With the explosion of globalization and the Internet, OSINT has become one of the fastest growing and most prolific sources of information. The real input for SLTP stakeholders in collection lies in HUMINT, especially in the case of law enforcement, and OSINT. The other disciplines are still cost prohibitive for most entities below the federal level. DHS advocacy on the part of SLTP will essential for the achievement of IP.

3. Processing and Exploitation

This step takes the raw information collected and renders it into a useful product. There is tension between the collection aspect of the intelligence cycle and processing. For primarily economic reasons, technical collection systems receive priority when it comes to budget and oversight. The result is imbalances between what is collected and what is actually processed. The volume of information to be processed into intelligence is simply too large to handle. Providing the IC with specific requirements can help reduce the amount excess information impeding proper exploitation and processing.

4. Analysis and Production

Analysts take the processed information and place it into the context of the requirement to produce an intelligence product. The ramifications of a particular piece of processed information can be different based on your perspective and/or responsibility. The difference between near and far fights or long versus short-term outlooks points to the need for tailored analysis. This is an area where the DHS can provide support to STLP by providing funds for local analysts or training and increased access to processed information existing local analysts. Funding, training, and access were all cited as impediments to effective integration by the STLP stakeholders interviewed for this thesis. Their concerns will be expanded upon in subsequent chapters.

5. Dissemination

Dissemination of the completed intelligence product occurs in two places, both within and without the producing organization. The internal dissemination poses only minor issues. Interagency circulation and distribution outside the IC are a key factors leading to intelligence failure. Dissemination problems range from traditional stovepipes, classification (trust issues), and cultural attitudes. Dissemination issues have given rise to numerous programs to mandate the sharing of information. The Information Sharing Environment (ISE)[44], as mandated by President Bush, is a key initiative in this area and will be discussed at length in this thesis. The sharing of information and ultimately intelligence is what underpins the national strategy for homeland defense. The DHS must work to break down dissemination barriers to support STLP stakeholders and make them equal partners in national defense.

6. Consumption

Consumption is nothing more than use of a particular intelligence product to support policy, strategic, or tactical goals. The ability of an agency to consume

[44] "Information Sharing Environment," http://www.ise.gov/ (accessed 10/3/2008).

intelligence is predicated on the timeliness and actionable nature of that intelligence. This goes back to properly defining requirements and disseminating them in manner that is useful. Barriers to consumption can include classification, sheer volume, or ignorance of what is available for consumption.[45] The DHS can help SLTP stakeholders at this stage by providing a means to discover what is available. This will allow consumption to be tailored to specific needs.

7. Feedback

The feedback loop is a critical component of any effective system. Feedback can occur at point in the intelligence cycle, so long as it does occur. Members of the IC often lament that they have no feedback on which to base their actions.[46] The DHS can play a critical role in acting as a liaison between SLTP stakeholders and the IC.

The intelligence cycle is a constantly in a state of flux with multiple steps happening simultaneously. The rapidly changing inputs and outputs of the system make it critical that STLP stakeholders are integrated into the process so they are not left behind to the detriment of national security.

D. BARRIERS

Several classes of barriers to the effective leveraging of intelligence support are civil liberties concerns, administrative issues, resource scarcity and corporate culture.

1. Civil Liberties

Civil liberty concerns are paramount in a democratic society, and an inherent distrust of secrecy is part of the American cultural narrative. The real argument here is freedom versus security. Benjamin Franklin was quoted as saying

---

[45] Scott Berg, Personal Interview by the author, 9/23/2008.

[46] Lowenthal, *Intelligence: From Secrets to Policy*, 64.

> Anyone who trades liberty for security deserves neither liberty nor security.[47]

These are strong sentiments, and they resonate both positively and negatively in American culture to such an extent that they will not be directly discussed in this thesis. The Thesis will instead focus on the areas where the DHS has a legitimate chance at effecting change. Following this line of thought, issues such as “posse comitatus” will not be addressed.

2. Classification

The classification of data is the number one impediment to intelligence proliferation. Even if all of the other barriers could be resolved, the inability to access the intelligence would still render it useless. A look at sensitive but unclassified information (SBU) gives us a snapshot of the problem. A GAO review of federal agencies revealed that 56 separate designations were given to SBU information, and 16 of these resided in a single organization (Department of Energy).[48] This is a single non-classified designation; when we add truly classified information to the mix, the waters become extremely muddy.

The number of designations is problematic, but so is the lack of overarching standards that allows for this type of latitude. There also needs to be a standard for granting clearances and mandated reciprocity across agencies. Under the current system, a clearance issued by the FBI may not be considered valid by the DOD and vice versa. This issue was addressed in 1991 with National Security Directive 63. NSD 63 stated that

> Investigations satisfying the scope and standards specified above are transferable between agencies and shall be deemed to meet the investigative standards for access to collateral Top Secret/National Security Information and Sensitive Compartmented

---

47 Benjamin Franklin, "Benjamin Franklin Quotes," http://www.brainyquote.com/quotes/quotes/b/benjaminfr384732.html (accessed 10/3/2008).

48 GAO, "GAO-06-385: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,"http://www.gao.gov/new.items/d06385.pdf (accessed 8/21/2008). table 2.

> Information. No further investigation or reinvestigation prior to revalidation every five years will be undertaken unless the agency has substantial information indicating that the transferring individual may not satisfy eligibility standards for clearance or the agency head determines in writing that to accept the investigation would not be in the national security interest of the United States.[49]

In short, what is good for one agency should be good for another. Two more Executive Orders, 12968 and 13381, and the IRTPA have made significant headway, but shortcomings still remain.

3. Administrative Issues

Standardization of procedures and training of personnel are low cost ways to mitigate risk. Standardization gives the right hand confidence that the left is doing the correct thing and facilitates integration across all levels. Representatives Howard Berman and Bennie Thompson roundly criticized the Bush administration for failing to implement the recommendations of the 9-11 commission. Some areas of failure are directly linked to DHS information sharing initiatives:

> Section 511 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) mandates the Department of Homeland Security (DHS) to issue a concept of operations for DHS State, Local, and Regional Information Fusion Center Initiative.[50]

The DHS failed to produce this document, and fusion centers continue to operate in an ad hoc fashion. This is their right as they are entities of the states or localities that formed them. However, the lack of standardization mandated makes it hard for the IC to integrate and achieve IP.

---

[49] George Bush, "NSD 63: Single Scope Background Investigations," http://www.fas.org/sgp/othergov/nsd63.html (accessed 10/19/2008).

[50] Bennie Thompson and Howard Berman, *Wasted Lessons of 9/11: How the Bush Administration has Ignored the Law and Squandered it's Opportunities to make our Country Safer*,[2008]), http://homeland.house.gov/SiteDocuments/HR1AnniversaryReport.pdf. 23.

Funding for analysts has been undermined by the structure of the DHS grant process. The current structure of the funding system only allows grant money to fund hiring, training, and retention of new and existing intelligence analysts for three years. This is an improvement of the previous periods, when the cap was set at two years. Arbitrary funding caps and time limitations on the use of funds has forced some States and localities to fire analysts after three years just to continue qualifying for DHS funding.[51] This exact problem has been cited as a significant roadblock in the city of Anaheim, CA and will be discussed in a later chapter.

4. Culture

The intelligence community was borne of the cold war, and as such its culture is one of secrecy, not only with respect to foreign governments but also across its own agencies and the tax paying constituency that funds it. This attitude is understandable given its historical context; however, understanding does not give way to advocating the broadcasting of secrets. That being said; there has to be a change in the mindset of the IC to facilitate national defense in a networked and globalized world. The solution then becomes the development of a corporate intelligence structure that nurtures an omni-directional flow of information embracing everyone whom has a legitimate stake in homeland defense. J.M. McConnell, the Director of National Intelligence, summed these concepts up succinctly when he said:

> …We must challenge the status quo of "need-to-know" culture and move to one of a "responsibility-to-provide" mindset.[52]

---

[51] Bennie Thompson and Howard Berman, *Wasted Lessons of 9/11: How the Bush Administration has Ignored the Law and Squandered it's Opportunities to make our Country Safer*,[2008]), http://homeland.house.gov/SiteDocuments/HR1AnniversaryReport.pdf. 27

[52] Office of the DNI, *United States Intelligence Community Information Sharing Strategy*, (2008), 2.

E. SUMMARY

This chapter has given a summary of the IC, how it works and some of the challenges faced when leveraging its assets to bolster the capabilities of SLTP stakeholders.

- The idea of Intelligence Proliferation was introduced, as a label to identify what success will look like. IP should not be taken to suggest unfettered access to intelligence. The concept is that those at the STLP level, whom have been properly vetted, will become integrated and equal partners in National Defense.
- The structure of the IC and its oversight regimes tends to "stove-pipe" information. The addition of SLTP partners, underpinned by information sharing will lead to a more networked structure that will bolster National Security.
- The traditional seven-step intelligence cycle can be an effective tool if the SLTP stakeholders can be integrated. I have suggested several areas that DHS can facilitate entry into this cycle by SLTP. The most important areas are in requirements generations and feedback.
- Areas that impede Intelligence Proliferation include classification, cultural and administrative issues.

The ground truth of these barriers is best illustrated by the experiences of SLTP stakeholders in their day-to-day operations. In order to frame the problem at the SLTP level, Chapter III will explore the attitudes of police chiefs and sheriffs in the state of California, as well as the specific experiences of Anaheim, California.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FRAMING THE PROBLEM: THE LOCAL PERSPECTIVE

As previously discussed, *The 9-11 Commission Report*, states that a failure to connect the dots contributed to the success of the 9-11 attacks. The implication is that the Intelligence community was unable to marshal its considerable resources to properly protect the nation. This raises more questions than it answers, chief among them is whether or not intelligence could have predicted the plot and subsequently foiled it. If so, then what was the nature of the failure and how do you solve it? This thesis suggests that the failure of integration that contributed to 9-11 is symptomatic of a larger problem. The root cause of the failure was and, to some extent, still is the structure of the IC.

A new environment of blurring borders and jurisdictional boundaries has called into question traditional roles and distinctions between domestic and foreign intelligence. The pre 9-11 IC was simply not adaptive enough to counter the asymmetrical threat that international terrorism posed. *Vision 2015*, the roadmap for the future of the IC as seen by the ODNI, states that:

> To respond effectively to the changing strategic landscape, we need structures, people and systems aligned to ensure a unified effort, ready to adapt with greater agility.[53]

The solution lies in the leveraging of federal intelligence assets and the integration of local law enforcement along with their private sector partners. The leveraging process can be achieved by any number of means. These means are the policies and programs discussed in this thesis that will lead to Intelligence Proliferation.

Which programs are appropriate for a given situation and how we know when an effective nexus of the IC and law enforcement communities has been achieved, will depend in large part on the attitudes and perceptions of the stakeholders, that is, do they perceive the value of the changes as worth the

[53] ODNI, "Vision 2015 Globally Networked Intelligence," http://www.dni.gov/Vision_2015.pdf (accessed 8/19/2008). 8.

expense. No group of stakeholders is going to agree 100% on a course of action or the efficacy of a resolution. This is due largely to the fact that any resolution can have effects beyond its original intent. In the case of the IC, any change in its complicated structure and the inclusion of new elements (SLTP stakeholders) is bound to have secondary and tertiary effects far in to the future. The structure of the IC after 1947 did not serve the nation well post cold war. Changes made to the IC to function post 9-11, may protect us in the short term, but set us up for failure against some as of yet unknown future threat. Any measures taken to change the IC will leave a mark at some point in the future. Not knowing the extent or duration of these effects makes the integration of previously unconnected organizations an area of concern.

A. SURVEY OF LAW ENFORCEMENT EXECUTIVES

The development strategy for an IC/LE nexus is confounded not only by the shadow of the future, but also by the perceptions of the stakeholders. Prior to 9-11, local law enforcement felt they didn't receive enough intelligence. The federal government felt that in many cases they (law enforcement) didn't have a need to know. Patrick Miller, a career police officer, conducted a survey of over 240 police chiefs and sheriffs in the state of California between 2004 and 2005. The results of his survey indicate that not much has changed since 2001.

Miller asked a series of six questions about the current state of information and intelligence sharing at the local level. He categorized the responses into four groups based on the relative size of the departments. Figure 1 (below) illustrates the responses from group two (departments with 100-500 sworn officers). I have chosen this group because it corresponds roughly to the size of the departments in Anaheim, California. Anaheim was the focus of interviews conducted along the same lines. Miller concluded, based on the survey of all four groups, that:

> …Across the board, local law enforcement agencies feel that there is inadequate information sharing and resources available to accomplish the homeland security mission.[54]

The survey was not all bad news; some distinct patterns emerged that point to a promising future, if the momentum for change can be sustained. The largest departments had the most favorable responses. By and large they felt that the training, technological enablers (in the form of databases), and access to daily intelligence briefs was adequate. The question of fusion center participation was embraced in an overall positive manner with over 92% of the respondents expressing interest.[55] The fall off in satisfaction seemed to have a causal relationship with decreasing size of departments. Intuitively this points to a need for targeted resource allocation to smaller departments, especially in the area of training, which showed the highest levels of dissatisfaction.

QUESTION	YES	NO
Is there adequate intelligence sharing between federal, state and local agencies?	22%	78%
Do you have adequate resources to accomplish your intelligence collection responsibility since Sept. 11th?	13%	87%
Has your agency received adequate training in intelligence/information sharing requirements?	13%	87%
Are your aware of the variety of Federal databases and information sharing technologies?	62%	38%
Do you receive daily, updated intelligence briefings?	31%	69%
Would you participate in a fusion center in your county?	89%	11%

Figure 1. Responses to Interview Questions, Group 2. This group consisted of 45 departments.[56]

---

[54] Patrick Miller, "How can we Improve Information Sharing among Local Law Enforcement Agencies?" (MA National Security Studies, Naval Postgraduate School), 46.

[55] Ibid., 46.

[56] Patrick Miller, "How can we Improve Information Sharing among Local Law Enforcement Agencies?" (MA National Security Studies, Naval Postgraduate School), 44.

Miller conducted a follow up with the 2005 survey respondents in 2007. The data showed a dramatic increase in the level of satisfaction across all sizes of departments except those with less than 50 sworn officers. In the case of group two departments, the perception of the adequacy of intelligence sharing doubled to 48%. The average of all departments in this category was 22% in 2005; the increase to 51% constitutes a statistically significant increase.[57] Clearly there is still work, but the results reinforce the patterns identified in the first survey. The one area that still shows a need for improvement is that of resource allocation. In 2007 there was still an 87% dissatisfaction rate with the amount of resources available to execute the intelligence-gathering portion of the homeland security mission.[58]

B. ANAHEIM CALIFORNIA

Miller's 2005 data reflected the evolution of perception amongst local law enforcement since 9-11. In order to gauge the continuity of that thought since 2005, and perhaps gain some insight into the ground truth of integration gaps, the interaction of the IC, law enforcement and first responders was explored in Anaheim California. In September 2008, several sit down interviews were conducted with representatives from Anaheim Fire and Police Departments. No federal representatives were available; however their lack of input makes the data more congruent with Miller's findings for comparative purposes. The following is a summary of the responses.

The first thing that is striking about the city of Anaheim is that they have a Homeland Security Battalion Chief on their organizational chart. What is even more interesting is that a professional fire fighter, Tim O'Hara, fills the position. This is not illuminating on the federal level, but it shows significant integration on the local levels. The city of Anaheim has broken down some significant cultural

---

[57] Patrick Miller, "The View of Law Enforcement Leaders in California: A Comparison of Perspectives between 2005 and 2007" (power point presentation of survey data, 2008).

[58] Patrick Miller, "The View of Law Enforcement Leaders in California: A Comparison of Perspectives between 2005 and 2007" (power point presentation of survey data, 2008).

barriers between fire and law enforcement and placed personnel in a joint command. This represents a change in paradigm over a relatively short period. The Anaheim Homeland Security Battalion (AHSB) did not even contain a reference to the fire department in 2002. In terms of integration with the law enforcement and the federal government the hierarchy was clear. The federal government was "assisted" by law enforcement, and fire was relegated to "cooperating" with both entities as directed. In 2006 there was finally integration of police and fire.[59] Chief O'Hara credited personal relationships at the executive level with breaking down the cultural barriers but he concedes that there is still work to be done:

> We still see pushback from the police, especially in the Terrorism Liaison Officer Program (TLO). At a recent training attended by over 100 people, I was the only fire officer; they asked why I was even there.[60]

The TLO program illustrates an integrated training opportunity for local entities. A successful graduate of the program will be able to use the exploratory techniques of Intelligence Led Policing to act as a conduit for the proliferation of terrorism information. In 2007 there were 50 TLOs in Orange County, and there has been an increase to 187 in 2008. Of this number, 11 are firefighters, and 40 more firefighters are slated for training next year.[61] There is discussion of the inclusion of private sector partners in the program. Critical infrastructure operators such as Disney are prime candidates due to their unique threat environment. Currently the intelligence analysts at Disney meet monthly with intelligence working groups in Anaheim.[62] The inclusion of private sector partners

---

[59] Tim O'Hara, Personal Interview by the author, September 15, 2008.

[60] Tim O'Hara, Personal Interview by the author, September 15, 2008.

[61] Jeff Van Der Sluys Veer, Personal Interview by the author, September 19, 2008.

[62] Scott Berg, Personal Interview by the author, September 23, 2008.

in training opportunities is an important avenue for integration and intelligence proliferation. The expansion in size and scope of the TLO program suggests that training is happening and barriers are being removed.

The AHSB is well versed in the use of available data systems. They find the Homeland Security Information Network (HSIN) particularly useful. Embedded in this system is a fire service intelligence exchange and emergency preparedness links that facilitate their use of intelligence. All parties interviewed also pass and receive information via the California Joint Regional Exchange System (CAL JRIES), tripwire, and the National Operations Center (NOC). The major complaint is the lack of access to secret data. The problem is characterized as two-fold, the lack of clearances and portals. The AHSB is located at a satellite office of the Anaheim police department. As of 2008 this building has no capacity for secret data portals. Currently the only secure portals are available at the Los Angeles Joint Regional Intelligence Center (LAJRIC). Timeliness of data is compromised by the average commute time of 1:30 minutes, one way, to access secret data. To date this has been more of an annoyance than operational problem, but it represents an information-sharing barrier that can be easily mitigated. The current systems are only functional if people are aware of them and use them. The experience of “stumbling” upon useful systems has caused frustration.. Chief O’Hara found the systems he uses by accident or word of mouth. This sentiment was echoed in other interviews. What is needed is a “menu” of available systems and their associated capabilities.[63] This would allow for specificity of information retrieval and efficient allocation of resources. The research suggests that some potentially helpful systems may be underutilized for no other reason than lack of publicity. The information sharing environment, as envisioned by its framers, will need to find ways to penetrate more deeply into the consciousness of SLTP stakeholders.

[63] Scott Berg, Personal Interview by the author, September 23, 2008.

Anaheim is still experiencing problems with the reciprocity of security clearances. Most of the AHSB have clearances issued by DHS. The DHS clearance is not well received by the local FBI or, in some cases, by local law enforcement who discriminate against fire. This problem may be more cultural than a case of policy. Chief O'Hara is the homeland security battalion chief for Anaheim. This fact is well known, and he is accorded due courtesy. Problems often arise at the LA JRIC. He recounted several experiences when his credentials were questioned because of his fire uniform. In one case he was denied access to secret data by the FBI, even after his clearance (from DHS) was validated. This was cleared up relatively quickly, but not without hurt feelings and harsh words.[64]

Fusion center participation is robust in Anaheim. They have personnel at the Orange County Intelligence Assessment Center (OCIAC) and the LA JRIC. The OCIAC has a local focus and serves as a collection and processing point for information gathered using the exploratory techniques of intelligence led policing. The OCIAC was formerly the Terrorism Early Warning Group; the reason for the change was not conveyed. The current organization is based on a fusion center model that is inclusive of law enforcement, fire, health, and the private sector, and it has adopted an all-hazards approach. The goal of the center is to improve interagency coordination, protect critical infrastructure, and analyze intelligence. The organization also serves as the primary disseminator of daily intelligence briefs.[65] The main difference between the OCIAC and other fusion centers is their ability and willingness to engage in "light surveillance."[66] Since 2003 the number of tips and leads the center has processed has increased from 111 per year to an average of 342. The LA JRIC serves the region and is where the interface with federal agencies takes place. The individual departments who detail their people to the centers, fund the participation. They would all like to do

64 Tim O'Hara, Personal Interview by the author, September 15, 2008.

65 Jeff Van Der Sluys Veer, Personal Interview by the author, September 19, 2008.

66 Ibid.

more, but funding is an issue. The three-year funding cap on analysts imposed by the DHS grant structure is an improvement over past systems. However, when the current grant cycle runs out, the local departments will not have the funding to retain them.[67]

A related problem to funding is resources in general. Integration has costs beyond personnel that must be addressed. Equipment needs and more mundane expenses, such as rent, must be addressed. Anaheim does not feel that they have been asked what they want, and they have no way of knowing what is available. The current requirements are being driven by a grant system, based on regulation, which dictates what departments can have, as opposed to what they need. Bolstering response will require funding structures tailored to individual needs, not the conjecture of someone 2000 miles away.[68]

The intelligence cycle is not currently being utilized as a model for generating intelligence in Anaheim. The people interviewed felt that the appropriate place for integration into the intelligence cycle was at regional rather than local fusion centers. The reasoning was that the OCIAC served the needs for specificity at the local level. They felt that federal level intelligence would be nothing but white noise at the local level, and the regional centers could act as the filters.

C. SUMMARY

The Miller data and the situation in Anaheim suggest that the attitudes of stakeholders are generally favorable regarding the cost benefit analysis of participation in information sharing. There are several roadblocks that must be addressed in order to integrate SLTP stakeholders with the federal government and achieve Intelligence Proliferation.

---

[67] Scott Berg, Personal Interview by the author, September 23, 2008.

[68] Scott Berg, Personal Interview by the author, September 23, 2008.

- There is perceived lack of resources. Resources take the form of funding, equipment and discoverability of data and programs to support intelligence integration.
- Cultural barriers impede the free flow of information.
- The value of the intelligence cycle is recognized, but not utilized to its full potential. The embracing of intelligence policing techniques across all levels will sustain a strong start for the fusion concept.
- Security clearance issues, particularly reciprocity, inhibit information exchange. This barrier is more cultural than statutory and needs to be addressed by strong leadership.
- Funding and grant structures do not fit local needs

Chapter IV of this thesis outlines policies and programs designed to target these specific issues and identify some of the most promising for further exploration.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POLICIES AND PROGRAMS

Because there is no consensus on what integration looks like, there is no limit on the number or nature of possible courses of action to develop a nexus of intelligence and law enforcement.

A. POLICIES AND PROGRAMS

The globalized threat environment, brought to the forefront of U.S. consciousness by the attacks of 9-11, continues to grow and evolve at a pace that cannot be matched by a cold war intelligence structure. Asymmetry and networked structures enable our enemies to rapidly assimilate new technologies and procedures without bureaucratic hindrance. Terrorists are free to train, reconnoiter targets, share information, and disseminate their message with little constraint. In order to counter this threat, the United States needs to move with purpose towards leveraging all elements of national power, especially intelligence. All of the major federal stakeholders in homeland defense have prepared policies and programs that outline the way forward. Many of these documents were prepared with the input of law enforcement agencies, such as the International Association of Chiefs of Police (IACP). Some civilian agencies, such as the Major Cities Chiefs Association (MCCA), prepared their own. What follows is a brief discussion of some of these major programs. Intelligence Led Policing, intelligence fusion, and data classification issues are the concerns that are addressed most often and point towards Intelligence Proliferation.

1. National Criminal Intelligence Sharing Plan

In 2002, the IACP held a summit on criminal intelligence information sharing. This summit gave birth to the Global Justice Information Sharing Initiative Intelligence Working Group. (GIWG) The GIWG teamed with elements within the DOJ to produce the National Criminal Intelligence Sharing Plan. (NCISP) The GWIG vision of what the plan should be included nine areas of focus.

- A model intelligence sharing plan
- A mechanism to promote the intelligence-led policing
- A blueprint for law enforcement administrators to follow
- A model for intelligence process principles and policies
- A plan that respects and protects individuals' privacy and civil rights
- A technology architecture to provide secure, seamless system information sharing
- A national model for intelligence training
- A plan that leverages existing systems and allows flexibility for advancements
- An outreach action plan to promote timely and credible intelligence sharing[69]

The size of departments has a direct impact on the amount of resources available for implementation. Because seventy-five percent of police departments have less that twenty-four sworn officers,[70] the 28 recommendations that grew from the nine vision areas were designed for maximum effectiveness regardless of size.

Recommendation one of the NCISP addresses the disparity in size and resources of departments. It advocates minimum standards of compliance and training with respect to Intelligence Led Policing and intelligence functions.[71] Compliance requires capital expenditure. In order to strengthen homeland security through ILP, the plan recommends funding across the board, specifically

---

69 GIWG Committee, *The National Criminal Intelligence Sharing Plan* Bureau of Justice Assistance,[2005]), http://it.ojp.gov/documents/NCISP_Plan.pdf. 10.

70 Ibid.

71 Ibid., 10.

in the areas of training and technological infrastructure. The fear is that without adequate funding, there will be a lack of implementation, and the country will remain at risk.[72]

Intelligence is not the exclusive property of law enforcement or the IC. The non-exclusive nature of intelligence makes it critical that private sector partners are engaged in any process. To this end the plan recommends the establishment of regular communication and engagement with private sector critical infrastructure for the purposes of information exchange.[73] Information exchange is hampered by the current classification system. Everyone recognizes the need to secure methods and sources; therefore the plan recommends technical means to expedite "tear line" products.[74] Recommendation twenty-four of the plan expands this further by advocating many technical enablers of information sharing that will be addressed later in the thesis.[75] If true sharing is going to occur, there is a level of trust that must be achieved across the spectrum of law enforcement and extended to include all appropriate stakeholders. The NCISP suggests extensive background checks for individuals with access to sensitive intelligence. These checks would include fingerprints and standard name records searches every three years.[76] The level of investigation is less than that of traditional security clearance and is only a suggestion of minimum standards.

The recommendations I have briefly described are by no means exhaustive of the entire plan. They do however give a snapshot of some of the early post 9-11 thought processes. The themes running through the NCISP will be repeated in subsequent efforts.

---

[72] GIWG Committee, *The National Criminal Intelligence Sharing Plan* Bureau of Justice Assistance,[2005]), http://it.ojp.gov/documents/NCISP_Plan.pdf. 11.

[73] Ibid., 13.

[74] Ibid., 17.

[75] Ibid., 23.

[76] Ibid., 25.

2. Law Enforcement Assistance and Partnership Strategy

The staff of the House Committee on Homeland Security prepared the *Law Enforcement Assistance and Partnership Strategy* (LEAP). The drafters of the document proceeded based on the assumption that, within their jurisdictions, local law enforcement was uniquely qualified to identify and thwart abnormal activity, which could be a precursor to terrorist activity:

> Accordingly, providing police and sheriffs' officers with the information and intelligence resources they need to make sense of what they encounter on the ground every day – and to share their observations and concerns with the federal Intelligence Community (IC) in response – would be a giant leap toward making the homeland more secure.[77]

The committee believed that information was not being properly shared and offered seven steps to that end. The steps included establishing of a national center for intelligence led policing, funding overseas liaison programs, establishing border intelligence fusion centers and associated funding, creating sanitized, law enforcement friendly intelligence products, expediting security clearances, and tracking the progress of these initiatives over time. The next section will explore some of the common themes in detail.

ILP is based on the premise that local police officers collect countless pieces of information that, if properly analyzed and aggregated, could be an invaluable intelligence tool. ILP has the dual benefit of serving not only counter terrorism, but also all crime mitigation. The committee believes that there are two major factors inhibiting the kind of ILP that supports national security. The first is the perception that intelligence is the purview of the federal government. The second is a lack of training and standards for the collection, consumption, and

[77] The Committee on Homeland Security, "Law Enforcement Assistance and Partnership Strategy," http://epic.org/privacy/fusion/leap.pdf (accessed 10/14/2008). 1.

privacy issues of intelligence.[78] Intelligence analysts have a separate concern as articulated by Lisa Palmeiri of the International Association of Law Enforcement Intelligence Analysts:

> Intelligence analysts and officers disseminate too much raw information, creating an environment of white noise…Vital information is still not accessible to law enforcement analysts at the state and local levels…law enforcement officers and executives are not trained consumers of intelligence.[79]

The LEAP strategy for the establishment of a National Center for ILP would address all of these concerns and problems. The particulars of these solutions will be investigated in a separate section on ILP contained in Chapter V.

The United States has 216 airports, 143 seaports and 115 land border crossings that serve as official points of entry into the country.[80] The federal agencies responsible for the ports of entry cannot be reasonably expected to catch everything. State and local law enforcement must be engaged to defend the spaces in between. The problem is a lack of technological interoperability and intelligence sharing. Everyone realizes that there is a problem, but the DHS has failed to develop a system of border intelligence sharing with its local partners. The lack of institutionalization has reduced the flow of information to a system based on personal relationships.[81] The ebb and flow of these relationships is not an effective strategy for national defense and borders on hope. LEAP advocates border fusion centers and the funding for their establishment and sustainment.

---

[78] The Committee on Homeland Security, "Law Enforcement Assistance and Partnership Strategy," http://epic.org/privacy/fusion/leap.pdf (accessed 10/14/2008). 6.

[79] The Committee on Homeland Security, "Law Enforcement Assistance and Partnership Strategy," http://epic.org/privacy/fusion/leap.pdf (accessed 10/14/2008). 7.

[80] Ibid., 14.

[81] Ibid., 15.

These fusion centers will serve to close the gaps between our ports of entry. Fusion centers and the issues associated with them will be addressed in Chapter V.

The Vertical Intelligence Terrorism Analysis Link (VITAL) is a program designed to mimic the United Kingdom's Joint Terrorism Analysis Centre (JTAC). The difference between JTAC and our National Counter Terrorism Center (NCTC) is the inclusion of local police via the Police International Counterterrorism Unit (PICTU). The PICTU gets the local under the same roof as the government operators and facilitates the flow of information and the break down of cultural barriers. VITAL would serve the same purpose at the NCTC. LEAP envisions detailed, properly cleared, local officers doing tours of duty at the NCTC. The locals could share their particular concerns about what affects them locally and work to convert classified documents to law enforcement friendly consumables.[82] The adoption of the LEAP plan and its funding can go a long way towards integrating locals into the intelligence cycle.

The flow of intelligence can be enhanced or blocked by the nature of ones security clearance. LEAP sees two overarching problems with the system of clearances in its current form, reciprocity and timeliness. The process of getting a clearance is backlogged, and in many cases it takes an inordinate amount of time to get a clearance complete. Once the process is complete many agencies don't recognize the validity of another department's clearance. For example the FBI doesn't recognize a clearance issued by DHS without further investigation.[83] LEAP proposes a program called MUSCLE (Moving Urgent Security Clearances for Law Enforcement). This program calls for the standardization of clearances for the purpose of reciprocity and mandates a sixty to one hundred twenty day processing time, depending on the level of clearance required.

---

[82] The Committee on Homeland Security, "Law Enforcement Assistance and Partnership Strategy," http://epic.org/privacy/fusion/leap.pdf (accessed 10/14/2008). 22.

[83] Ibid., 26.

LEAP advocated funding overseas liaison officers and benchmarking processes to assess the current state of affairs. While foreign exchange may be of benefit to large metropolitan areas, this is an appropriate expenditure of funds given the size (less than 24 sworn officers) of most departments and jurisdictions. Research shows no evidence that the benchmarking process/survey suggested in 2006 has occurred or will ever occur. Many of the other programs suggested by LEAP have made preliminary strides towards fruition with the introduction of S.3524, the Homeland Security and Law Enforcement Improvements Act of 2008. Senator Joe Biden of Delaware introduced the bill September 18, 2008. It has been referred to the House Committee on Homeland Security, the same committee that authored LEAP.

3. Information Sharing Strategy

On February 22, 2008, The Office of the Director National Intelligence (ODNI) issued the *United States Intelligence Community Information Sharing Strategy.* J.M. McConnell, the Director National Intelligence, summed up the goals of the strategy as follows:

> Together we must challenge the status quo of 'need to know' culture and move to one of a 'responsibility to provide' mindset. Implementing this strategy will enable intelligence entities to act as stewards of intelligence data and take advantage of every opportunity to share information that can improve the security of our Nation.[84]

Much like "intelligence", information sharing means different things based on relative positional perspective within the overall system. The ODNI strategy is predicated on their position at the top of the information sharing hierarchy. They define information sharing as:

> …Information sharing behavior is the act of exchanging intelligence information between collectors, analysts, and end users in order to

[84] Office of the DNI, *United States Intelligence Community Information Sharing Strategy*, 2.

> improve national and homeland security. Information providers must make information accessible, available and discoverable at the earliest point possible.[85]

There are several key take-a-ways from this definition. The most important is the verbiage that makes information sharing an explicit behavior, not a passive phenomenon. Further this behavior occurs between individuals at all levels of the intelligence cycle. Therefore, the strategy defines itself as a behavior not a technology and is inclusive not exclusive. This way of framing the way forward should help break down the cultural impediments to intelligence proliferation.

The strategy itself is broken down into four strategic goals and numerous linked strategic objectives. The goals articulate what should happen and the objectives identify the path to the desired final condition. Finally the implementation is linked to the *500 Day Plan.* Figure 2 below outlines the goals.

STRATEGIC GOAL	DESCRIPTION
GOAL #1: Institute Uniform Information Sharing Policy and Governance	Enable the transformation of culture necessary for information sharing policies, governance models, standards, personnel evaluation and awards, and compliance mechanisms.
GOAL #2: Advance Universal Information Discovery and Retrieval	Advance information search, discovery, retrieval, dissemination and pervasive connectivity through common meta-data tagging,, security markings, and networks throughout the Intelligence Community.
GOAL #3: Establish a Common Trust Environment	Put in place uniform identity attributes, identify management, information security standards, information access rules, user authorization, auditing , and access control to promote common trust.
GOAL #4: Enhance Collaboration Across the Community	Develop the tools and incentives necessary at the institutional, leadership, and workforce levels to collaborate and share knowledge and expertise and information.

Figure 2. Strategic Goals[86]

The goals were designed to be achievable and measurable without overstepping the bounds of realistic probability. The objectives associated with each goal attempt to clearly articulate 'deliverables' for each area, thus

[85]Office of the DNI, *United States Intelligence Community Information Sharing Strategy*, 3.

[86] Office of the DNI, *United States Intelligence Community Information Sharing Strategy*,12.

establishing metrics for evaluation. Articulation of metrics is where the document loses momentum. For instance the third goal (Establish a common trust environment) contains five objectives.

- Define a uniform structure and attributes to enable identity management and the guidance to support decentralized agency specific implementation.
- Establish Identity management standards, to include authorization, authentication, auditing and cross-domain services.
- Develop information security policies that support data protection efforts.
- Create a common classification guide for the IC.
- Establish an approach that manages risk, supports trust and protects sources and methods.[87]

Each of these objectives depends on the development or establishment of new policy or is contingent upon implementation of the same. In short, any one of the objectives is a single point of failure for the entire enterprise. The objectives are attainable, but they will require more than legislation or the programming of new policies and procedures. They will require a shift in culture, and management cannot mandate a cultural shift. The question of implementation has been addressed by linkage to the *500-Day Plan for Integration and Collaboration*. The plan outlines the deliberate ways the IC is moving towards transformation, and it is divided in six areas of focus. Figure 2 (below) shows how the strategic goals are linked to specific areas of the plan.

[87] Office of the DNI, *United States Intelligence Community Information Sharing Strategy*,14.

STRATEGIC GOAL	500 DAY PLAN
GOAL #1: Institute Uniform Information Sharing Policy and Governance	Core Initiative: Update policy documents clarifying and aligning intelligence community authorities. Initiative 5B: Collaborate to protect privacy and civil liberties. Initiative 6E: Harmonize intelligence community policy on "US Person" information.
GOAL #2: Advance Universal Information Discovery and Retrieval	Initiative 2A: Create a single information environment. Initiative 2B: Implement attribute-based access and discovery.
GOAL #3: Establish a Common Trust Environment	Initiative 2B: Implement attribute-based access and discovery. Initiative 2D: Establish a single community classification guide. Initiative 5D: Improve information technology certification & accreditation process.
GOAL #4: Enhance Collaboration Across the Community	Core Initiative: Create collaborative environment for all analysts. Initiative 2C: Provide collaborative information technology to federal executive department agencies and organizations. Initiative 2D: Establish a single community classification guide.

Figure 3. Plan Linkages[88]

The information sharing strategy and the 500-Day Plan are both products of the IC and designed at their core to address issues within the traditional IC. Initiatives One and Two of the 500-Day Plan (create a culture of collaboration and accelerate information sharing) contain clauses that speak directly to the engagement of non-federal partners. In order to address this direct linkage, the ODNI has established a steering committee to coordinate efforts with other information sharing initiatives. One of the initiatives alluded to in the 500-Day Plan is *Vision 2015.*

4. Vision 2015

The office of the Director National Intelligence published *Vision 2015* in 2008 to expound upon the intelligence enterprise first introduced in the National

[88] Office of the DNI, *United States Intelligence Community Information Sharing Strategy*,16.

Intelligence Strategy. It calls for a globally networked and integrated Intelligence Enterprise for the 21st century, based on the principles of integration, collaboration, and innovation.[89] The document does not explicitly mention SLTP stakeholders as partners, but rather calls for the involvement of "numerous new partners."[90] The goal of the vision articulated in the document is decision advantage. Decision advantage is simply the leveraging of all available intelligence assets and partners to acquire and provide an informational edge and to deny our adversaries the same. The five facets of the plan are customer driven intelligence, global awareness and strategic foresight, mission focused operations, net centric information enterprise, and enterprise integration. Enterprise integration is the lever that will enable full partnership of SLTP stakeholders and facilitate intelligence proliferation.

a. Enterprise Integration

Vision 2015 requires a strong core foundation. This foundation is comprised of the vital elements of the intelligence enterprise: people, processes and technology. The organizations of the IC historically have had problems managing these areas:

> Organizational differences, competing cultures, non-interoperable systems, unclear decision rights and conflicting business rules acted as barriers to collaboration, greatly undermining our ability to adapt and reducing our organizational agility…we will need continued leadership and organizational commitment to truly integrate by 2015.[91]

The ODNI continues to work towards the institutionalization of information sharing and has instituted an incentive structure that spans the entirety of the intelligence enterprise. A key change along these lines is the requirement of "joint" duty for promotion to senior executive levels within the six

---

[89] ODNI, *Vision 2015 Globally Networked Intelligence.*

[90] ODNI, *Vision 2015 Globally Networked Intelligence* 4.

[91] Ibid., 15.

departments under the purview of the DNI.[92] The goal of this policy is to develop leaders who can rise above parochialism and build relationships that foster true collaboration.

The transformation of security functions is a key component of integration. The enterprise will function on common security standards and practices that will be designed to support new partners. The new security environment will require some fundamental changes to the classification system. The trick will be simplification without compromise.

The agility of infrastructure will also need to be addressed:

> By 2015, employees from different agencies will have to be collocated to more remote locations, away from centralized headquarters. The needs for cross-organizational collaboration, cross-functional teams and programs will require a more agile infrastructure.[93]

The concept of agility to support collaboration suggests the type of arrangement seen in state fusion centers and the NCTC. If true collaboration is to be achieved, mitigation of cultural, monetary, and bureaucratic frictions, as well as a lack of focus has to be addressed across all five facets of the plan. The first and foremost of these barriers is cultural. When it comes to implementation we:

> …Are challenging an operational model of this vision that worked, and proponents of that model will resist change on the basis that it is unnecessary, risky or faddish.[94]

Once the cultural barriers are removed via strong transitional leadership, the forward progress of the vision will be able to move towards the resolution of the other issues.

---

[92] ODNI, *Vision 2015 Globally Networked Intelligence* 15.

[93] ODNI, *Vision 2015 Globally Networked Intelligence* 16.

[94] Ibid., 22.

B. THE NATIONAL STRATEGY

The preceding section has shown just a few of the numerous plans around the nation and across all levels of government. The National Strategy for Information Sharing is the effort of the federal government to articulate and memorialize the full contours of disparate strategies into a single document.[95] The subtitle of the document is “Successes and Challenges in Improving Terrorism-Related Information Sharing”; this underscores the importance of information sharing as the centerpiece of national security. The plan outlines five foundational elements. Sharing amongst federal agencies, SLT entities, private sector, and foreign partners account for the first four. The fifth is the protection of privacy and other related legal rights. Foreign partners and legal issues are outside the scope of this project; the others will be discussed in turn.

1. Information Sharing at the Federal Level

There are five generally recognized communities within the federal government that are targeted by information sharing strategies. The IC, homeland security, law enforcement, defense, and foreign affairs will work within a framework established by the plan in order to achieve interagency cooperation. The cooperation at the federal level is a template to be applied at all other levels. The NCTC is of particular interest, as it deals specifically with intelligence and national defense. In theory all federal entities that acquire or posses terrorism related information would provide that information to the NCTC for analysis, processing and dissemination. The Interagency Threat Assessment and Coordination Group (ITACG) is responsible for sanitizing the intelligence for distribution outside the federal government.

---

[95] National Security Council, "National Strategy for Information Sharing," http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf (accessed 10/17/2008). 1.

2. Information Sharing with State, Local and Tribal Entities

The primary mission of local law enforcement and first responders is not counter-terrorism. This emerging mission must be integrated into current responsibilities without overstretching resources and breaching the trust of their communities. These local concerns change the perspective from which the problem of national security, and support needed to achieve it, is viewed.. SLTP entities must develop a culture of fusion; this is an all crimes approach that includes the identification of a possible nexus of local crime and national security implications. There must also be situational awareness across all levels of government. SLTP must send information up the chain for analysis, and the IC must reciprocate. The key to this relationship is collaboration, the onus for advancing this collaboration lies with the federal government. The ITACG is a primary conduit for collaboration of 'tear line' products. These products however do not answer the need for clearances of SLTP. There is still a need for key stakeholders at the SLTP level to have access to the same raw data at their fusion centers in order to gain the advantage of the local perspective before further dissemination and data customization as deemed appropriate. It is the policy of the strategy to

> …Promote state and major urban area fusion centers to achieve a baseline level of capability and become interconnected with the Federal government and each other, thereby creating a national, integrated, network of fusion centers to enable the effective sharing of terrorism related information.[96]

C. INFORMATION SHARING WITH THE PRIVATE SECTOR

The private sector is involved with national security primarily through its ownership of 85% of the critical infrastructure in the United States and its responsibility to protect it. The National Infrastructure Protection Plan outlines

[96] National Security Council, "National Strategy for Information Sharing," http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf (accessed 10/17/2008). 20.

specific ways the federal government interfaces with CI owners and operators. The NSIS supports the NIP by advocating the inclusion of CI into the intelligence cycle and the common operating picture as appropriate.

D. SUMMARY

There are several recurring themes in each of the plans presented.

- There is a universally recognized need for the fusion of information at all levels of government. The appropriate venue for the aggregation of information and resources is the fusion center.
- Collaboration implies a flow of information across all axes. The best facilitator of this flow is the movement to a networked organizational structure.
- First responders, be that police, fire, or rescue, are invaluable sources of terrorism information and mitigation. They must be supported through the leveraging of all assets of national power, especially timely, locally targeted, and actionable intelligence.
- The exploratory nature of Intelligence Led Policing makes it the construct for information gathering and shows the most promise for exploiting the nexus of crime, terrorism, and national defense.
- Implementation of any policy will have to overcome cultural barriers and build an environment of trust.

These common themes are addressed through ILP and fusion centers. In order to facilitate intelligence proliferation and national defense, ILP will gather the information, and fusion centers will act as the conduit between SLTP and the IC/DHS. Both will be discussed in detail in Chapter V.

THIS PAGE LEFT INTENTIONALLY BLANK

V. IMPLEMENTAION OF PROLIFERATION

Chapter IV identified areas of overlap that are common to all of the disparate strategies and programs. There is a universally recognized desire for intelligence fusion, a networked structure, the inclusion of first responders and private sector partners, the techniques of ILP as a facilitator of intelligence, and the breakdown of cultural barriers. The focal point for change comes from these areas of overlap. Large scale buy-in by all the stakeholders is made easier by the leverage of common concerns. Machiavelli in his book *The Prince* framed the difficulties of implementation as follows:

> There is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things.[97]

The new order is the integration of STLP stakeholders, and the difficulty lies in the perception, bolstered by a cold war attitude, that intelligence is a close hold and secrecy is paramount. Because conventional wisdom was fraught with the distrust of people and agencies outside ones own, intelligence was dispensed on a strictly need to know basis. In order for Intelligence Proliferation to be successful, a shift in paradigm to a responsibility to provide will be necessary. The way to achieve this shift is by focusing on areas of agreement and designing implementation strategies that demonstrate the value and engender the trust of all stakeholders. With the inclusion of STLP stakeholders, the fundamental architecture of intelligence functions will change from “stove piped” to “networked”. This new, networked architecture will facilitate an Information Sharing Environment (ISE). The ISE underpins Intelligence Led Policing techniques, which will provide the exploratory information necessary for Fusion Centers.

---

[97] Niccolo Machiavelli, "Niccolo Machiavelli Quotes," http://www.brainyquote.com/quotes/quotes/n/niccolomac131418.html (accessed 11/5/2008.

A. UNDERPINNINGS

1. Networked Approach

Secretary Chertoff addressed the first annual National Fusion Center Conference in March 2007. His message was that the intent of the federal government was not to create a single fusion center controlled by the government, but rather:

> …A network of centers all across the country, a network which is visible not only to the federal level, but as important, if not more important visible to each of you working in your own communities so you can leverage all the information gathered across the country to help you carry out your very important objectives.[98]

The network architecture of which Secretary Chertoff spoke is important and bears further discussion. The threat caused by terrorism is unlike any the United States has dealt with in the past. Our military and security apparatus is designed to counter threats posed by other nations. These traditional threats are above board and can be handled in a variety of ways, both with known counterparts and the backing of the international community. In short, national security occurs at the macro level. Intelligence structures and functions tend to be agency specific and focus on other states. Divination of secrets and the security of our own secrets create stovepipes that compartmentalize information. These informational stovepipes are a primary factor in intelligence failures. The al-Qaeda operatives who perpetrated the 9-11 attacks did not so much exploit these stovepipes as benefit post facto from their existence. The end result is the same and highlights deficiency in the current structure. We can look to our enemies to see the solution.

An asymmetrical terrorist group uses a networked structure to operate unhindered at the micro level. The typical terrorist network is scale free as opposed to random. What this means is that the terror cells (groups) are fairly dense (well connected to each other). In this sense, the terrorist cell is much like

---

[98] Rollins, *Fusion Centers: Issues and Options for Congress*, 10

the stove piped architecture we are trying to mitigate. However, central individuals bridge the cells of a scale free network. This structure has two implications for counter-terrorism and by extension Intelligence Proliferation. First, attacking the cell itself will not disrupt the entire network; in fact destroying an individual terrorist cell will have little overall effect on the network as a whole. The disruption of scale free networks requires attacking the few well-connected individuals who form the bridges and hold the network together. For example, the well-connected nodes in a random network are connected to an average 27% of all other nodes within the network. The connection rate in a scale free network of the same size is almost 60%.[99] The reason terror networks are effective is the connectivity and resilience evidenced in their scale free construct. The second implication is that for national defense to be effective, we need to strive for the same connectivity that our enemies exploit. To do this we must first share information. To achieve this goal, information sharing will form the links that connect disparate organizations and is critical to the formation of networks.

2. Information Sharing Environment

Congress and President mandated the Information Sharing Environment (ISE) through section 1016 of the IRTPA. This section directed the facilitation of sharing information of value to combat terrorism. The ISE strategy for accomplishing this goal is grounded in existing systems and technologies, rather than the creation of a new domestic intelligence regime. The alignment and leveraging of existing policies, processes, technologies, and systems will potentially lead to a culture of collaboration.[100] The culture of collaboration envisioned by the ISE has many characteristics of a network. It will be resilient, sustainable, and adaptable. These traits will be important to support the five

---

[99] "QuickStudy: Scale-Free Networks," http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html (accessed 10/31/2008).

[100] ODNI, "Information Sharing Environment," http://www.ise.gov/index.html (accessed 10/31/2008).

communities the ISE serves: intelligence, law enforcement, defense, homeland security, and foreign affairs. The vision statement of the ISE is to develop:

> A trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States by the effective and efficient sharing of terrorism and homeland security information.[101]

The ISE vision recommends specific responsibilities on the part of all stakeholders. There are four roles that are specific to SLTP stakeholders: fostering a culture of fusion, maintaining situational awareness, protecting critical infrastructure, and developing terrorism specific training. Each of these areas is to be addressed with the help and consultation of federal partners.

The culture of fusion enumerated in the ISE refers to fusing of crimes data with data affecting national security. ISE is not bound by a single federal agency or component; it is a broad-based coordination and collaboration effort among various stakeholders. [102] Thus, fusion will have to be a collaborative process that has input about crime from STLP partners and national security data from federal partners. Determining what applies to each specific jurisdiction and the nation will require the integration of SLTP stakeholders into the intelligence cycle as equal partners. Integration requires inputs and a place, physical or virtual, for the intelligence cycle to manifest itself. The inputs will come from the techniques of ILP, and a place for these goals to be accomplished will come from an integrated national network of fusion centers.[103] Fusion at the national level is already occurring at the National Counter Terrorism Center (NCTC), and their analysis is being disseminated via the Interagency Threat Assessment and Coordination

---

[101] ODNI, "Information Sharing Environment," http://www.ise.gov/index.html (accessed 10/31/2008).

[102] GAO, "GAO 08-492: Information Sharing Environment, Definition of the Results to be Achieved in Improving Terrorism-Related Information Sharing is Needed to Guide Implementation and Assess Progress," http://www.gao.gov/new.items/d08492.pdf (accessed 11/8/2008).33

[103] ODNI, *Information Sharing Environment*

Group. Research suggests that dissemination is occurring to some extent. AHSB personnel reported getting intelligence products from a number of sources including the ITACG. The main issue of concern from their standpoint was applicability at the local level. This suggests that a local model can be extended to SLTP as the common ground that will lead to Intelligence Proliferation.

B. INTELLIGENCE LED POLICING

1. Background

Intelligence Led Policing is different from traditional law enforcement in that it attempts to prevent crime, not solve and prosecute after the fact. This methodology of crime prevention has been used to some extent in community oriented policing endeavors. Community Oriented Policing (COP) builds rapport with local communities by developing a continuity of relationships that focuses on specific needs. The ongoing positive interaction with police builds trust and turns a formerly adversarial relationship into one characterized by fruitful interaction. This leads to increased situational awareness and a keen sense of impending problems or anomalies with in the community. There is collaboration between the local community and law enforcement that leads to lower crime and higher satisfaction. ILP is the next logical link in the chain after COP. Community oriented policing seeks to act locally, while the concept of ILP embraces the broader problems of multi-jurisdictional crimes and terrorism. Integration of formal intelligence functions into police work serves two purposes. The first is tactical; appropriate intelligence products can be used to prevent crimes such as terrorism and identify the protection needs of critical infrastructure. To a lesser extent, it can also be used to solve crimes and prosecute offenders, but this is the traditional role of the police and doesn't represent a radical departure from the norm. The second role of ILP is strategic. The situational awareness characteristic of a functioning intelligence apparatus can lead to a proactive, targeted application of increasingly dwindling resources. The processing of information into the intelligence products that define the value of ILP occurs

through integration into the intelligence cycle. The value of integration into this cycle is recognized in the various programs discussed in this thesis and is supported by the research conducted with stakeholders in Anaheim California.

2. Benefits

The design and implementation of ILP is complicated, but the benefits are simple and profound. The police become a link between the local communities and the intelligence apparatus. The officers grow to be a two-way conduit for threat information between the local community and the intelligence apparatus. The situational awareness that comes from the intelligence apparatus can be fused with what is happening on the streets in order to identify possible precursor crimes or impending terrorist activity. The informed officers can put information into context on the streets, while the information gathered by those officers can help higher levels of government put local events into context at their level. The omni-directional flow of information that ILP generates facilitates Intelligence Proliferation and ultimately national defense.

3. Barriers

ILP is the exploratory collection of information needed to feed local and regional intelligence cycles while being sensitive to the perceptions and civil rights of the communities in which they work. The American Civil Liberties Union (ACLU) takes issue with the fusion of law enforcement activities and domestic intelligence. A December 2007 report by the ACLU stated that:

> There is a long, nasty history of abuse surrounding vaguely defined, proactive “intelligence” as carried out by domestic law enforcement agencies at the local, state and federal level…Urban police have long maintained political intelligence units, which spied upon and sabotaged numerous peaceful groups in utterly illegal ways.[104]

---

[104] Michael German and Jay Stanley, "What's Wrong with Fusion Centers," American Civil Liberties Union, http://www.aclu.org/privacy/gen/32966pub20071205.html (accessed 10/31/2008). 7.

A specific area of concern is the disposition of collected data. There is the fear that data, once collected, will be kept, even if no crime has been committed. This could very well lead giant databases that could be "mined" to the detriment of the law-abiding public. This and other civil liberty concerns will have to be addressed for effective implementation. Failure to do so will result in a loss of trust between law enforcement the communities they are charged to serve.

A larger issue, at least from a practical standpoint, is the funding and training requirements generated by the addition of an intelligence function. Surveys and interviews conducted pursuant to this thesis indicate a high degree of dissatisfaction with the funding and training support available to local entities. The Miller survey data shows that 78% of the respondents felt resources were inadequate and 74% reported the same deficiencies in training.[105] To be sustainable, ILP must have the buy in of those who control budgets. To do so will require demonstration of results and the nexus between local conditions and national security.

Nested in the budget issue is analysis. Most departments cannot afford to hire their own intelligence analysts. This makes them dependent on products and information developed by outside agencies. The content of proper intelligence products is often of limited use owing to a lack of locally targeted context. Often times it is only a deluge of non-specific information. The Anaheim Homeland Defense Battalion relies primarily on the OCIAC for their products to mitigate this phenomenon.[106] The *IACP Intelligence Sharing Report* cites the need to address analysis as the chief barrier to implementing ILP. The IACP says we must find ways to:

---

[105] Miller, *How can we Improve Information Sharing among Local Law Enforcement Agencies?*, 43-45.

[106] Personal interview by author, September 23, 2008.

> …Place a higher value on true analysis, support analyst positions and provide the opportunity for analysts to effectively engage in the intelligence mission.[107]

A final barrier to the implementation of ILP is the disaggregation of systems designed to support the intelligence cycle. In order for information sharing to lead to Intelligence Proliferation, the technical enablers must share compatibility. It will do no good to overcome cultural and structural issues only to have our desire to communicate hampered by a “Tower of Babel” exchange structure.

ILP is essentially the adoption of the intelligence cycle for SLTP stakeholders. This definition suggests points of entry for the DHS to act as facilitators in the implementation process. The DHS must be prepared to act as liaisons between the SLTP stakeholders and the IC. The inclusion of stakeholders into the intelligence cycle will be particularly important in the areas of requirements generation and feedback. A major contribution of the DHS is funding. There must be a critical review of grant policies and procedures to ensure the distribution of funds meets the needs of SLTP entities and the intent of national defense. At issue is the continuity of funds. It does no good to predicate a large portion of the national defense on the participation of SLTP stakeholders, and then cut off the funds that sustain them. SLTP stakeholders should not receive a free ride. They will need to adopt an all hazards strategy that justifies the expense of programs beyond terrorism. This is why ILP is important, it makes local communities safer and bolsters national defense. The Global War on Terror has been described as “The Long War”. The DHS should be prepared to fund SLTP stakeholders until either local fiscal support is secure or the long war is won.

---

[107] IACP, "Criminal Intelligence Sharing: A National Plan for Intelligence Led Policing at the Local, State and Federal Levels," http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf (accessed 11/2/2008). IV.

C. FUSION CENTERS

1. Background

The strength of American law enforcement lies in its decentralized nature. The specialization and local knowledge enjoyed by individual jurisdictions, with their own tailored way of doing business, far exceeds any level of excellence that could be achieved with a single national structure. When other first responders and private sector entities are leveraged, the pervasive nature of the resultant structure forms the safety net that allows local communities to function. Unfortunately in the post 9-11 globalized world, this local focus and sheer number of agencies inhibits the integration needed to combat asymmetrical threats. The primary reason that decentralization has become a weakness is that local communities are very integrated, but that's where it stops. The IC and its SLTP partners are a collection of agencies, not a system. The 9-11 commission report cited a further disparity in the nations intelligence function, that of the divide between domestic and foreign intelligence:

> Foreign intelligence agencies were watching overseas, alert to threats from foreign interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States.[108]

The divide in intelligence roles caused a simple but profound effect on the outcomes of 9-11. The only people with a chance to interact with the bombers were STLP stakeholders, but no one told them who or what to look for. The responsibility for failure doesn't lie with any individual or organization, but rather with the system as a whole. A fusion center can be the lens that focuses disparate organizations into a cohesive system in order to avoid a repetition of this past failure.

Intelligence functions are not new to law enforcement. Metropolitan areas have had intelligence units for many years. The fusion center concept has grown

---

[108] Thomas Kean and others, *9-11 Commission Final Report*,[2004]) (accessed 8/20/2008). 263.

dramatically since 9-11. A perceived lack of intelligence support from the federal government led many states to stand up their own intelligence structures. The federal government has come to see the value of SLTP fusion centers and has taken steps to leverage these organizations for the mutual good of all involved. Local law enforcement and other stakeholders have been enlisted to become the eyes and ears of communities in the war on terror. With the proper training and support, local communities can be the vital link that sustains the nation in a time of war. The appropriate venue for this training and support is the “Fusion Center.”

> A fusion center is defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.[109]

2. Benefits

The benefit of fusion center lies in the simple premise that the more information is shared, the more potential intelligence is developed. Because this is true, intelligence development becomes self-sustaining through this virtuous circle. The fusion center becomes the focal point for omni-directional information flow, bolsters the intelligence cycle for all stakeholders, and leads to intelligence proliferation. The DHS sees four discrete of benefits arising from fusion centers. These benefits are applicable to all stakeholders participating in the fusion process.

- Clearly defined information gathering requirements
- Improved intelligence analysis and production capabilities
- Improved information and intelligence sharing
- Improved prevention, protection, response and recovery capabilities[110]

Additionally there are benefits that apply primarily to the DHS, and others that are most applicable to state and local stakeholders.

---

109 "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," http://www.iir.com/global/ncisp.htm (accessed 9/2/2008). 2.

110 Rollins, *Fusion Centers: Issues and Options for Congress*, 4.

Benefits to DHS

- Improved situational awareness
- Improved access to local officials
- Access to non-traditional sources
- Improved informational flow from the SLTP to DHS

Benefits to Stakeholders

- Clearly defined DHS entry point
- Insight into federal priorities
- Participation in threat dialogue
- Increased onsite intelligence expertise
- Improved information flow from DHS[111]

The OCIAC is functional example of a local fusion center that meets some of these criteria, but falls short of complete integration.

3. Barriers

Fusion center success is predicated on the inclusion of all stakeholders. The need for an all hazards approach to demonstrate viability and secure continuity of funding calls for the inclusion of stakeholders across all levels of government, first responders and appropriate members of the private sector (particularly owner operators of critical infrastructure). Who these stakeholders are will vary from location to location. While there will be a preponderance of law enforcement personnel in the fusion centers, as most centers are evolutions of existing law enforcement intelligence organizations, a sustainable fusion center is not a law enforcement fusion center.

The Congressional Research Service (CRS) has published several extensive reports on fusion centers. The most recent one, published in January 2008, suggests that underlying philosophy is an issue and the current guidelines do little to mitigate this issue. The guidelines have the following limitations: (1) they are voluntary (2) the philosophy outlined in them is generic and does not

[111] Rollins, *Fusion Centers: Issues and Options for Congress*, 4.

translate theory into practice, and (3) they are oriented to the mechanics of fusion center establishment.[112]It has been suggested that fusion centers have perhaps developed too quickly with disregard for the underlying discipline of intelligence fusion.[113] For fusion to occur and the center to become more than window-dressing, real transformation must occur at the organizational level. All of the stakeholders need to agree on a common philosophy of proactive approaches to terrorism and crime, responsibility for security, and environmental understanding to discern threats.[114] The question becomes one of benefits. This is defined by who is included and should therefore pay the tab.

The costs of fusion centers are a major concern, and where those costs are borne is a particularly salient issue. The support of the DHS to state run centers consists primarily of financial assistance through grant programs that totaled almost $240m in FY08[115]. The longevity of this funding cannot be counted on; so the value of fusion centers will again have to be proven through an all hazards/all stakeholders approach.

A possible barrier to the sustainability of fusion centers is time. If there are no major terrorist attacks in the next decade or so, fusion centers that dedicate themselves to counter terrorism will have outlived their usefulness. The perceived lack of need will eventually outweigh the costs, and finances will be redirected. Since we all agree that terrorism is anathema to polite society, catastrophic events to justify the existence of a center are not desirable. Fusion centers will indeed have to become all hazards organizations. They will need to embrace natural and man-made disasters, as well as crime, to prove their worth as the memories of 9-11 fade.

---

[112] Rollins, *Fusion Centers: Issues and Options for Congress*, 10.

[113] Ibid., 10.

[114] Ibid., 10.

[115] DHS, *State and Local Fusion Centers.*

Fusion centers must ensure the privacy of our citizens. The ACLU has published a document that identifies some characteristics of fusion centers as potential civil liberties pitfalls. They believe that fusion across all levels of government leads to “policy shopping” or the use of whichever policy is less restrictive in a multi jurisdictional environment.[116] Although this flexibility can be problematic, adherence to the provisions of Title 28 of the CFR part 23[117] mitigate this concern. The inclusion of private sector partners and first responders, such as emergency medical technicians, also raises privacy concerns. There is the fear that information gathered by these entities in the course of their day-to-day duties could be stored and data mined. The ACLU premise that intelligence gathered in the absence of criminal predicate is unlawful resonates within the IC and SLTP stakeholders. DNI, Mike McConnell has wrestled with this issue and stated the following:

> The intelligence community has an obligation to better identify and counter threats to Americans while still safeguarding their privacy. But the task is inherently a difficult one.[118]

Fusion centers will have to be especially diligent to avoid losing the criminal predicate when handling sensitive personal data. Furthermore, they must make sure that new STLP partners have the training necessary to avoid civil rights violations and possible litigation.

The DHS must take the lead to break down the barriers to fusion center success and act as a liaison and facilitator for SLTP stakeholders. In order to do this there must both a monetary and physical presence. The DHS has addressed this by committing both personnel and resources to fusion centers. As of March 2008, there were 58 operational intelligence fusion centers in the United States

---

[116] German and Stanley, *What's Wrong with Fusion Centers*, 10.

[117] Title 28 CFR part 23 governs the ways that personal data can be stored and exchanged by law enforcement.

[118] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs,* July/August, 2007http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html (accessed 11/2/2008).

receiving some sort of intelligence support from the DHS.[119] This evolved somewhat of late with the fielding of DHS personnel to limited sites. As of March 2008, there were 23 intelligence officers assigned to fusion centers with more in the pipeline.[120] These officers will act as the liaisons to facilitate the intelligence cycle. Furthermore, the DHS needs develop a common lexicon and training standards so that a network of fusion centers can interact across lines. There has to an arbiter amongst the agencies involved in the centers. As a relatively new entity the DHS must act as an honest broker to facilitate trust among the participants.

D. SUMMARY

If intelligence proliferation is to be achieved, the way forward is to construct a national intelligence regime that embraces the omni-directional sharing of information as prescribed by the Information Sharing Environment.

- Implementation strategies must focus on areas of overlap. The solution space defined by this overlap transitions the sharing of information from a negative to positive sum game.
- This regime will be networked as opposed to stove-piped. A network structure is necessary to practice counter terrorism at the "micro" level.
- Fusion center success is predicated on the inclusion of all appropriate stakeholders. The inclusive nature will facilitate an all hazards approach that will demonstrate value and facilitate continuity of funding.
- The fusion centers will act as the place where the information generated by Intelligence Led Policing enters the intelligence cycle and acts as the feedback loop for the dissemination and modification of the resultant intelligence.
- ILP is not the exclusive purview of law enforcement. It is a technique for the leveraging of all SLTP stakeholders.

---

[119] DHS, *State and Local Fusion Centers.*

[120] DHS, *State and Local Fusion Centers.*

- Funding and civil liberties concerns will have to be addressed if fusion centers are going to be sustainable.
- DHS is the natural choice for being the honest broker to facilitate fusion centers.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. CONCLUSIONS AND FINAL THOUGHTS

This thesis has shown that the need to proliferate intelligence to all appropriate levels of society is an imperative that was all too vividly illustrated by the attacks of 9-11. Terrorism cuts across all levels of society through loss of life, economic chaos, and the inhibition of freedoms. The horrific loss of life cannot be minimized or discounted, but the damage goes further, and its effects are enduring. Estimates of the future economic impact of terrorism, based on 9-11 losses, range from 100 million to 100 billion dollars per year.[121] These numbers don't quantify the emotional toll or the self-imposed loss of personal freedom that attacks the very nature of democracy. The prolific nature of terror calls for an equally prolific response. This thesis has argued that in order to best leverage intelligence support for SLTP stakeholders, all aspects of the intelligence enterprise must leveraged to form a collaborative intelligence community that includes federal, state, and local law enforcement as well as private sector partners. The policies and programs examined identify information sharing as the chief enabler of leverage. The premise is that the more information is shared the more intelligence is produced. This positive relationship drives the concept of intelligence proliferation.

The first part of the thesis gave a summary of the IC, how it works, and some of the challenges it faces when leveraging its assets to bolster the capabilities of SLTP stakeholders. The idea of Intelligence Proliferation was introduced, as a label to identify what success will look like. IP should not be taken to suggest unfettered access to intelligence. The concept is that those at the STLP level, who have been properly vetted, will become integrated and equal partners in National Defense.

---

[121] Gregory F. Treverton, "Reorganizing U.S. Domestic Intelligence: Assessing the Options," Rand Corporation, http://www.rand.org/pubs/monographs/MG767/ (accessed 11/11/2008).

In order to frame the problem at the SLTP level, this thesis explored the attitudes of police chiefs and sheriffs in the state of California. A survey of 243 law enforcement executives, conducted by Chief Pat Miller of the Ventura, CA police department, as well as the specific experiences of the Anaheim California Homeland Security Battalion served as the case studies. The Miller data and the situation in Anaheim suggest that the attitudes of stakeholders are generally favorable with regards to the cost benefit analysis of participation in information sharing. There are several roadblocks that must be addressed in order to integrate SLTP stakeholders with the federal government and achieve Intelligence Proliferation. The overriding concerns identified by this thesis research include the following:

- There is perceived lack of resources. Resources take the form of funding, equipment and discoverability of data and programs to support intelligence integration.
- Cultural barriers impede the free flow of information.
- Implementation of any policy will have to overcome cultural barriers and build an environment of trust.
- Security clearance issues, particularly reciprocity, inhibit information exchange. This barrier is more cultural than statutory and needs to be addressed by strong leadership.
- The value of the intelligence cycle is recognized, but not utilized to its full potential. The embracing of intelligence policing techniques across all levels will sustain a strong start for the fusion concept.
- There is a universally recognized need for fusion of information at all levels of government. The appropriate venue for the aggregation of information and resources is the fusion center.
- Collaboration implies a flow of information across all axes. The best facilitator of this flow is the movement to a networked organizational structure.
- The exploratory nature of Intelligence Led Policing makes it the construct for information gathering that shows the most promise for exploiting the nexus of crime, terrorism and national defense.

First responders, whether police, fire, or rescue, are invaluable sources of terrorism information and mitigation. By including state, local, and private sector parties in national defense, you empower them to be part of something bigger.

After 9-11 everyone wanted to do something, but there was a lack of focus. Inclusion of locals will build trust and rapport and help channel locally available resources. In the case of national defense, that resource is over 700,000 local police officers. They must be supported through the leveraging of all assets of national power, especially timely, locally targeted, and actionable intelligence. I believe that these common themes are addressed through ILP and fusion centers. ILP will gather the information, and fusion centers will act as the conduit between SLTP and the IC in order to facilitate intelligence proliferation and national defense.

Intelligence proliferation represents an innovation in the way information is converted to intelligence and is consumed to bolster national defense. The key lies in the implementation or “how to” stage of the process. The implementation stage of innovation is dangerous, because any paradigm shifting idea will result in the destruction of some part of the status quo. This destruction threatens stakeholders in the old regimes. These stakeholders must either buy into the plan or be marginalized for the plan to go into action and result in innovation. Intelligence proliferation aims to become the new status quo. If we can implement truly omni-directional information sharing across all levels of government, then the output should be a robust intelligence capability that is positioned to detect, deter, and prevent future terrorist activity. All implementation strategies must result in this output, the nature of the implementation will define the outcomes.

Information is power. Intelligence takes informational power and multiplies it, increasing its power by orders of magnitude. The proliferation of intelligence is the proliferation of power, and it is this power that will be at the core of national security in an asymmetrical world.

THIS PAGE LEFT INTENTIONALLY BLANK

BIBLIOGRAPHY

" Bureau of Justice Statistics Law Enforcement Statistics." http://www.ojp.gov/bjs/lawenf.htm (accessed 9/17/2008).

" Department of the Treasury." http://www.treasury.gov/ (accessed 9/5/2008).

" QuickStudy: Scale-Free Networks." http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html (accessed 10/31/2008).

"Bureau of Intelligence and Research." http://www.state.gov/s/inr/ (accessed 9/5/2008).

"Defense Intelligence Agency." http://www.dia.mil/ (accessed 9/5/2008).

"Department of Homeland Security | Preserving our Freedoms, Protecting America." http://www.dhs.gov/index.shtm (accessed 6/12/2008).

"Drug Enforcement Administration." http://www.usdoj.gov/dea/index.htm (accessed 9/5/2008).

"Federal Bureau of Investigation Homepage." http://www.fbi.gov/ (accessed 9/5/2008).

"Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era." http://www.iir.com/global/ncisp.htm (accessed 9/2/2008, 2008).

"Information Sharing Environment." http://www.ise.gov/ (accessed 10/3/2008).

"National Geospatial-Intelligence Agency." http://www1.nga.mil/Pages/Default.aspx (accessed 9/5/2008).

"National Reconnaissance Office." http://www.nro.gov/ (accessed 9/5/2008).

"National Security Agency." http://www.nsa.gov/about/ (accessed 9/5/2008).

"Secure Fence Act of 2006." http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6061enr.txt.pdf (accessed 6/12/2008).

"United States Intelligence Community." http://www.intelligence.gov/1who.shtml (accessed 9/5/2008).

108th US Congress. "Intelligence Reform and Terrorism Prevention Act of 2004." http://www.nctc.gov/docs/pl108_458.pdf (accessed 9/5/2008).

Berg, Scott. *Personal Interview*. Vol. Interview with Chief Scott Berg of the Anaheim Ca. Fire Department 2008.

Bush, George W. "Comments upon Signing H.R. 3199, USA Patriot Improvement and Reauthorization Act of 2005." http://www.whitehouse.gov/infocus/patriotact/ (accessed 10/1/2008).

Bush, George W. "Weekly Compilation of Presidential Documents." *Weekly Compilation of Presidential Documents* 37, no. 44 (November 5, 2001): 1561.

Bush, George. "NSD 63: Single Scope Background Investigations." http://www.fas.org/sgp/othergov/nsd63.html (accessed 10/19/2008).

Carafano, James. "Safeguarding America's Sovereignty: A "System of Systems" Approach to Border Security." http://www.heritage.org/research/homelandsecurity/bg1898.cfm (accessed 3/7/2008).

DHS News Release. "DHS Strengthens Intel Sharing at State and Local Fusion Centers." http://www.dhs.gov/xnews/releases/press_release_0967.shtm (accessed 6/19/2008).

DHS. "Information Sharing & Analysis." http://www.dhs.gov/xinfoshare/ (accessed 9/5/2008).

DHS. "State and Local Fusion Centers." http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed 9/17/2008).

DHS. "US-VISIT Program." http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed 4/26/2008).

DOE. "Department of Energy - National Security." http://www.doe.gov/nationalsecurity/ (accessed 9/5/2008).

Federal Register. "FR Doc E8-8956 ." http://edocket.access.gpo.gov/2008/E8-8956.htm (accessed 5/9/2008) 73 Number 80).

Franklin, Benjamin. "Benjamin Franklin Quotes." http://www.brainyquote.com/quotes/quotes/b/benjaminfr384732.html (accessed 10/3/2008).

GAO. "GAO 08-492: Information Sharing Environment, Definition of the Results to be Achieved in Improving Terrorism-Related Information Sharing is Needed to Guide Implementation and Assess Progress." http://www.gao.gov/new.items/d08492.pdf (accessed 11/8/2008).

GAO. "GAO-06-385: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information." http://www.gao.gov/new.items/d06385.pdf (accessed 8/21/2008).

German, Michael and Stanley, Jay. "What's Wrong with Fusion Centers." American Civil Liberties Union. http://www.aclu.org/privacy/gen/32966pub20071205.html (accessed 10/31/2008).

GIWG Committee. *The National Criminal Intelligence Sharing Plan* Bureau of Justice Assistance, 2005.

Global Security. "US-Mexico Border Fence: Great Wall of Mexico." http://www.globalsecurity.org/security/systems/mexico-wall.htm (accessed 3/8/2008).

Homeland Security. *Statement of Assistant Secretary Charles E. Allen.* 2007.

IACP. "Criminal Intelligence Sharing: A National Plan for Intelligence Led Policing at the Local, State and Federal Levels." http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf (accessed 11/2/2008).

Kean, Thomas, Lee Hamilton, Richard Ben-Venesti, Bob Kerry, Fred Fielding, John Lehman, Jamie Gorelick, Timothy Roemer, Slade Gorton, and Fred Thompson. *9-11 Commission Final Report*2004.

Lahneman, William. "The U.S. Intelligence Community." https://www.chds.us/coursefiles/NS4156/lectures/intel_us_intel_comm/player.html (accessed 9/5/2008).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 3rd ed. Washington DC: CQ Press, 2006.

Machiavelli, Niccolo. "Niccolo Machiavelli Quotes." http://www.brainyquote.com/quotes/quotes/n/niccolomac131418.html (accessed 11/5/2008).

McConnell, Mike. Overhauling Intelligence. *Foreign Affairs,* July/August, 2007.

Miller, Patrick. "How can we Improve Information Sharing among Local Law Enforcement Agencies?" MA National Security Studies, Naval Postgraduate School, 2005.

Miller, Patrick. "The View of Law Enforcement Leaders in California: A Comparison of Perspectives between 2005 and 2007." power point presentation of survey data.

Murphy, Laura W. "American Civil Liberties Union : Letter to the Senate Urging Rejection on the Final Version of the USA PATRIOT Act." http://www.aclu.org/natsec/emergpowers/14401leg20011023.html (accessed 10/1/2008).

Naim, Moises. "The Five Wars of Globalization." *Foreign Policy* no. January (2003): 29.

National Commission on Terrorist Attacks Upon the United States. *Statement to the National Commission on Terrorist Attacks upon the United States.* 2003, http://govinfo.library.unt.edu/911/hearings/hearing1/witness_ranstorp.htm (accessed 6/12/2008).

National Governors Association. "EC-05 Homeland Security Policy." http://www.nga.org/portal/site/nga/menuitem.8358ec82f5b198d18a278110501010a0/?vgnextoid=2a6a9e2f1b091010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD (accessed 6/19/2008).

National Security Council. "National Strategy for Information Sharing." http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf (accessed 10/17/2008).

NGA Center for Best Practices. "2006 State Homeland Security Directors Survey." http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf (accessed 6/19/2008).

ODNI "Information Sharing Environment." http://www.ise.gov/index.html (accessed 10/31/2008).

ODNI. "Vision 2015 Globally Networked Intelligence." http://www.dni.gov/Vision_2015.pdf (accessed 8/19/2008).

Office of the DNI. *United States Intelligence Community Information Sharing Strategy*2008.

O'Hara, Tim. *Interview*. Vol. Interview with Chief Tim O'Hara of the Anaheim Ca. Fire Department2008.

Rollins, John. "Fusion Centers: Issues and Options for Congress." http://www.fas.org/sgp/crs/intel/RL34070.pdf (accessed 11/2/2008).

The Committee on Homeland Security. "Law Enforcement Assistance and Partnership Strategy." http://epic.org/privacy/fusion/leap.pdf (accessed 10/14/2008).

Thompson, Bennie and Howard Berman. *Wasted Lessons of 9/11: How the Bush Administration has Ignored the Law and Squandered it's Opportunities to make our Country Safer*2008.

Treverton, Gregory F. "Reorganizing U.S. Domestic Intelligence: Assessing the Options." Rand Corporation. http://www.rand.org/pubs/monographs/MG767/ (accessed 11/11/2008).

United States Congress. "National Security Act of 1947." http://www.intelligence.gov/0-natsecact_1947.shtml (accessed 9/5/2008,).

Van Der Sluys Veer, Jeff. *Interview*. Vol. interview conducted at the Orange County Intelligence Assessment Center2008.

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California